



SysTechDev 2026

INTERNATIONAL CONFERENCE ON SECURE SYSTEMS
DESIGN AND TECHNOLOGY DEVELOPMENT

NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI"
ESTONIAN UNIVERSITY OF LIFE SCIENCES
VIDZEME UNIVERSITY OF APPLIED SCIENCES
GREEN FUTURE TECHNOLOGIES

SECURE SYSTEMS DESIGN AND TECHNOLOGY DEVELOPMENT (SysTechDev)

International Conference Proceedings
25-26 June 2026

VOLUME III



Veliko Tarnovo, Bulgaria 2026

NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI"

ESTONIAN UNIVERSITY OF LIFE SCIENCES

VIDZEME UNIVERSITY OF APPLIED SCIENCES

GREEN FUTURE TECHNOLOGIES

Proceedings of the International Conference
**Secure Systems Design and Technology
Development (SysTechDev)**
25–26 June 2026

Volume III

Veliko Tarnovo, Bulgaria
2026

Secure Systems Design and Technology Development (SysTechDev). Proceedings of the 1st International Scientific Conference, June 25–26, 2026. *Volume III*. National Military University "Vasil Levski", Veliko Tarnovo, Bulgaria, 2026. 415 pp.

The three-volume proceedings of the 1st International Scientific Conference "Secure Systems Design and Technology Development (SysTechDev)" present the latest research in defense and security technologies, engineering sciences and production technologies, information technologies, sustainable energy engineering and applications, laser technologies, materials science, mechanics, metalworking, mathematical modelling, and electrical engineering.

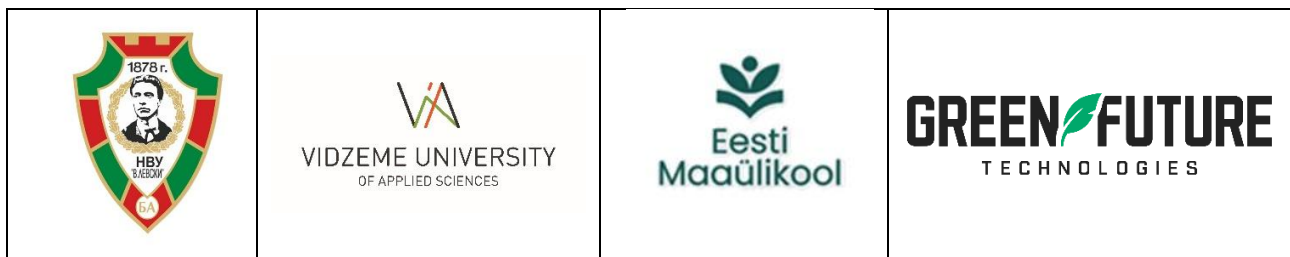
The conference is interdisciplinary, bringing together the achievements of international research teams. The scope of the studies presented in these proceedings is broad and multidisciplinary, reflecting the results of collaborative research conducted by scientists from different countries.

The conference proceedings include 196 scientific papers, with participants representing 16 countries.

The 1st International Scientific and Practical Conference on Secure Systems Design and Technology Development (SysTechDev) took place at the National Military University "Vasil Levski" in Veliko Tarnovo, Bulgaria, on June 25–26, 2026.

<https://etrconf.eu/>

Link to conference proceedings: <https://journal.etrconf.eu/std/issue/archive>



This journal is licenced under
[Creative Commons Attribution 4.0 International \(CC BY 4.0\) License](https://creativecommons.org/licenses/by/4.0/)
The author of the paper takes responsibility for the content of the paper



Online ISSN 3044-7771

Published by Green Future Technologies SIA, 2026

Scientific Committee Co-Chairman

Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
Dr.sc.ing. Artis Teilāns, Vidzeme University of Applied Sciences, Latvia

Scientific Committee

PhD Sherif Ibrahim Abdel-Wahab, Agricultural Research Center, Giza, Egypt
PhD prof. Tamer Ibrahim Abdel-Wahab, Agricultural Research Center, Giza, Egypt
PhD prof. Hikmat Almadhkhori, Al-Mustansiriyah University, Baghdad, Iraq
PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria
PhD Kiril Anguelov, Technical University of Sofia, Bulgaria
PhD Andres Annuk, Estonian University of Life Sciences, Estonia
PhD Ekaterina Arabska, Higher School of Agribusiness and Regional Development, Bulgaria
PhD Wael Badawy, International Atomic Energy Agency, Egypt
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Plamen Bogdanov, University of Library Studies and Information Technologies, Bulgaria
PhD Hamid Can, Trakya University, Turkey
PhD Arnis Cīrulis, Vidzeme University of Applied Sciences, Latvia
PhD Dimitar Dimitrov, Todor Kableskov University of Transport, Bulgaria
PhD Nadezhda Dimova, New Bulgarian University, Bulgaria
PhD Tamar Dolbaia, Tbilisi State University, Georgia
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Nino Durglishvili, Tbilisi State University, Georgia
Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Riga Technical University, Latvia
PhD Gilbert-Rainer Gillich, University Babes-Bolyai, Romania
PhD Grigor Grigorov, "Vasil Levski" National Military University, Bulgaria
PhD Mariusz Gontarczyk, Military University of Technology, Poland
PhD Tzvetelin Gueorguiev, Technical University of Gabrovo, Bulgaria
PhD Alexandru Herciu, „CAROL I” National Defense University, Romania
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Valery Ivanov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria
DSc Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
Dr.sc.ing. Aivars Kaķītis, Latvia University of Life Sciences and Technologies, Latvia
PhD Georgi Kamarashev, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
Dr.paed. Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Atis Kapenieks, Riga Technical University, Latvia
Dr. paed. Janis Kapenieks, Riga Technical University, Latvia
PhD Stancho Kajkov, "Vasil Levski" National Military University, Bulgaria
PhD Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain
PhD Noah Ugur Kilinc, Piri Reis University, Istanbul, Turkey
PhD Georgi Komitov, Agricultural University Plovdiv, Bulgaria
PhD Lazar Lazarov, "Vasil Levski" National Military University, Bulgaria
Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria

PhD Wilmer Orlando López González, Universidad Nacional de Educación, Ecuador
 PhD Tatyana Maglyovana, National University of Civil Protection of Ukraine, Ukraine
 Dr.sc.math. Maksims Marinaki, University of Latvia, Latvia
 PhD Rumen Marinov, "Vasil Levski" National Military University, Bulgaria
 PhD Georgi Marinov, Rakovski National Defence College, Bulgaria
 PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria
 PhD Otakar Jiří Mika, Police Academy and South Bohemian University, Czech Republic
 PhD Gregg Tyler Milligan, University of Canton, United States
 PhD Cristian Emil Moldoveanu, Military Technical Academy "Ferdinand I", Romania
 Dr.sc.ing. Marufjon Musaeu, Tashkent State Technical University, Uzbekistan
 PhD Serhii Naida, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
 PhD Nikolay Nichev, Georgi Benkovski Higher Military Air School, Bulgaria
 PhD Plamen Pavlov, School of Telecommunications and Posts, Bulgaria
 Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria
 PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
 PhD Prof. Vesela Radovic, University of Belgrade, Serbia
 PhD Tomas Rozsypal, University of Defence, Czech Republic
 PhD Rashmi Jaymin-Sanchaniya, Riga Technical University, Latvia
 PhD Yehya A. Salih, Head of Department at University of Basrah, Iraq
 PhD Iryna Sarancha, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Ukraine
 PhD Barbara Sawicka, University of Life Sciences in Lublin, Poland
 PhD Dafinka Sidova, New Bulgarian University, Bulgaria
 Dr.sc.ing. Andris Skromulis, Rezekne Academy of Riga Technical University, Latvia
 Dr.sc.ing. Adiljan Suleymanov, Tashkent State Technical University, Uzbekistan
 Dr.-Ing. Bambang Soemardiono, Institut Teknologi Sepuluh Nopember, Indonesia
 Dr.sc.ing. Artis Teilāns, Vidzeme University of Applied Sciences, Latvia
 PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia
 Dr.biol. Rasma Tretjakova, Rezekne Academy of Riga Technical University, Latvia
 PhD Antonios Valamontes, Research Director at Kapodistrian Academy of Science, United States
 PhD Sergij Vambol, National Technical University, Kharkiv Polytechnic Institute, Ukraine
 PhD Viola Vambol, University of Yuri Kondratyuk Poltava Polytechnic National University, Ukraine
 PhD Valentin Vassilev, New Bulgarian University, Bulgaria
 PhD Algazy Zhauyt, Almaty University of Power Engineering and Telecommunications, Kazakhstan
 Dr.sc.ing. Inga Zinicovscaia, Horia Hulubei National Institute for Physics and Nuclear Engineering, Romania

Organising Committee Chairman

PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria

Organising Committee

Aigars Abrickis, Green Future Technologies SIA, Latvia
 MA Yanitsa Boyanova, "Vasil Levski" National Military University, Bulgaria
 Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
 MA Georgi Hristov, "Vasil Levski" National Military University, Bulgaria
 PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia
 MA Svetoslav Pashunov, "Vasil Levski" National Military University, Bulgaria

Reviewers

PhD Andres Annuk - Estonian University of Life Sciences, Estonia
PhD Dimitar Angelski, Forestry Technical University, Bulgaria
PhD Svilena Arabadzhieva, Academy of the Ministry of Interior, Bulgaria
PhD Plamen Atanasov, New Bulgarian University, Bulgaria
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Daniel Berchev, "Vasil Levski" National Military University, Bulgaria
PhD Rosen Bogdanov, "Vasil Levski" National Military University, Bulgaria
PhD Olga Borisova, Varna Free University Chernorizets Hrabar, Bulgaria
PhD Erol Buyukliev, Rakovski National Defence College, Bulgaria
PhD Arnis Cīrulis, Vidzeme University of Applied Sciences, Latvia
PhD Aija Cunska, Vidzeme University of Applied Sciences, Latvia
PhD Iveta Daugule, University of Latvia, Latvia
PhD Dilyana Dimitrova, Nikola Vaptsarov Naval Academy, Bulgaria
PhD Desislava Dimitrova, Technical University of Varna, Bulgaria
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Kliment Georgiev, Technical University of Sofia, branch Plovdiv, Bulgaria
PhD Pēteris Grabusts, Riga Technical University, Latvia
PhD Aleksandrs Gorbunovs, Riga Technical University, Latvia
PhD Iliayn Hutov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo", Bulgaria
PhD Martins Jansevskis, Vidzeme University of Applied Sciences, Latvia
PhD Oskars Java, Vidzeme University of Applied Sciences, Latvia
PhD Sandra Kaija, Riga Stradiņš University, Latvia
PhD Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Atis Kapenieks, Riga Technical University, Latvia
PhD Kiril Lengerov, TU Sofia, branch Plovdiv, Bulgaria
PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria
PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria
PhD Ventsislava Nikolova-Minkova, Technical University of Gabrovo, Bulgaria
PhD Daniela Pavlova, University of Library Studies and Information Technologies, Bulgaria
PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria
PhD Penyo Penev, "Georgi Benkovski" Bulgarian Air Force Academy, Bulgaria
PhD Desislava Petrova, Technical University of Gabrovo, Bulgaria
PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
PhD Hristo Radev, Technical University of Gabrovo, Bulgaria
PhD Zhaneta Savova, National Military University, Bulgaria
PhD Dafinka Sidova, New Bulgarian University, Bulgaria
PhD Krasimir Slavyanov, "Vasil Levski" National Military University, Bulgaria
PhD Milko Stefanov, Rakovski National Defense College, Bulgaria
PhD Ivan Tashev, Technical University Sofia, branch Plovdiv, Bulgaria
PhD Tsvetoslav Tsankov, Konstantin Preslavsky University of Shumen, Bulgaria
PhD Kostadin Trifonov, University of Transport Todor Kableshev, Bulgaria
PhD Valentin Vassilev, South-West University "Neofit Rilski", Bulgaria
PhD Stoyan Vergiev, Technical University of Varna, Bulgaria
PhD Beata Vlahova, National Military University Vasil Levski, Bulgaria
PhD Emil Yankov, University of Ruse, Bulgaria
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria

Volume III

CONTENTS

Information Technology

Evgeni Andreev, Desislava Valcheva AN APPROACH FOR PREVENTING OVERLOAD OF THE EC2 SERVICE	13-17
Ralitsa Angelova-Slavova, Dimitar Tsvetkov ON SOME PROPERTIES OF POSTERIOR PREDICTIVE DISTRIBUTIONS	19-22
Ralitsa Angelova-Slavova, Dimitar Tsvetkov SOME PROPERTIES OF THE DIRICHLET TYPE INTEGRALS	23-26
Valentin Atanasov, Daniel Denev AN OPTIMIZED MODEL FOR CPU LOAD EVALUATION IN THE EXECUTION OF CODE STRUCTURES AND SCRIPT-BASED ALGORITHMS	27-32
Ivelina Balabanova, Desislava Petrova, Georgi Georgiev WEB TRAFFIC MANAGEMENT BY TECHNIQUES WITH SUPPORT VECTOR MACHINE, NAÏVE BAYES AND DISCRIMINANT ANALYSIS	33-38
Ansis Ataols Bērziņš TWO DECADES OF BALTIAN-LATGALIAN ELECTRONIC DICTIONARY	39-43
Angela R. Borisova, Krasimir Slavyanov REAL-TIME NETWORK TRAFFIC CAPTURE AND ANALYSIS USING A DEEP NEURAL NETWORK	45-52
Dmytro Dashenkov, Serhii Smelyakov, Anastasiya Chupryna IMPROVING TEXT SEARCH MEMORY EFFICIENCY WITH NSW TEXT INDEXING	53-57
Gergana Dimcheva, Ivaylo Stoyanov DETERMINING THE ORGANIZATIONAL LEVEL OF DIGITAL MATURITY FROM THE INTEGRATION OF AI IN THE SERVICE SECTOR IN THE REPUBLIC OF BULGARIA	59-65
Dimitar Dimitrov, Todor Balabanov, Irena Petrova APPLYING A HEURISTIC APPROACH TO TIME OPTIMIZATION IN A GRID SCHEDULE	67-72
Dimitar Dimitrov, Krassimir Lalov, Ivan Manchev, Irena Petrova CYBERSECURITY THREATS IN INTELLIGENT TRANSPORT SYSTEMS: CHALLENGES AND SOLUTION PATHWAYS	73-81
Peter Grabusts, Jurijs Musatovs EVALUATION OF THE PERFORMANCE OF CLASSIFICATION ALGORITHMS IN THE QGIS SYSTEM	83-89
Boris Gramchev, Marina Marinova-Stoyanova DECISION-MAKING DYNAMICS IN SECURE SOFTWARE DEVELOPMENT TEAMS: THE ROLE OF AI- SUPPORTED SYSTEMS	91-98

Rosen Iliev, Svilen Neykov GENERALIZED NET MODEL OF THE DISASTER PROTECTION ASSESSMENT PROCESS USING ARTIFICIAL INTELLIGENCE	99-105
Sandra Kaija, Inga Kudeikina ELECTRONIC EVIDENCE IN CRIMINAL AND CIVIL PROCEEDINGS: TECHNOLOGIES, CHALLENGES AND PERSPECTIVES	107-113
Svilen Kamdzhlov, Dimitar Nikolov CYBER THREAT INTELLIGENCE BASED SCOPING OF RED TEAM EXERCISES	115-119
Svitlana Kizim, Oksana Voloshyna, Liudmyla Bondarchuk, Svitlana Nahorniak, Olena Stoliarenko HUMAN CAPITAL DEVELOPMENT IN WAR AND POST-WAR TIMES USING ARTIFICIAL INTELLIGENCE	121-125
Nikolay Koev, George Dimitrov, Daniela Pavlova, Nikolay Penev A CONCEPTUAL MODEL FOR INFORMATION SECURITY ASSESSMENT IN JUDICIAL INFORMATION SYSTEMS BASED ON RISK AND REGULATORY REQUIREMENTS	127-132
Renata Kondratavičienė ARTIFICIAL INTELLIGENCE USE IN PROFESSIONAL BACHELOR THESIS WRITING: A SURVEY-BASED ANALYTICAL FRAMEWORK	133-139
Mariia Liashenko, Kirill Smelyakov, Anastasiya Chupryna, Dainius Savulionis, Loreta Savulioniene, Paulius Sakalys METHODS AND MODELS FOR IMAGE ENHANCEMENT IN LOW-LIGHT CONDITIONS	141-146
Kiril Luchkov ASSESSMENT OF THE DIGITAL MATURITY OF ESG REPORTING IN THE CONTEXT OF DIGITALIZATION	147-151
Oleksandr Malykhin, Nataliia Aristova, Liudmyla Dybkova COMPUTER SCIENCE STUDENTS' PERSPECTIVES ON INCORPORATING DIGITAL STORYTELLING FOR DEVELOPING CRITICAL THINKING SKILLS IN ENGLISH CLASSROOM	153-158
Oleksandr Malykhin, Nataliia Aristova, Liudmyla Dybkova STUDENTS' PERCEPTIONS OF USING AI INSTRUMENTS IN DEVELOPING LEARNING-TO-LEARN SKILLS: AN EXPLORATORY QUALITATIVE STUDY	159-163
Marina Marinova-Stoyanova, Boris Gramchev HUMAN-AI COLLABORATION IN SECURE SYSTEM DEVELOPMENT: DECISION PROCESSES AND ORGANIZATIONAL IMPLICATIONS	165-172
Penka Markova, Georgi Markov AI-ENHANCED DETECTION OF ARP SPOOFING-BASED MAN-IN-THE-MIDDLE ATTACKS IN LOCAL AREA NETWORKS	173-179
Penka Markova, Georgi Markov PERFORMANCE AND RESILIENCE ANALYSIS OF GRE OVER IPSEC TUNNELS IN DYNAMIC ROUTING NETWORKS	181-188

Stela Mincheva, Veselka Stoyanova THE RELATIONSHIP BETWEEN VISUAL STYLE AND EMOTIONAL ENGAGEMENT IN MOBILE TOURISM APPLICATIONS	189-194
Julija Mironova, Viktoriia Riashchenko, Baiba Rivža, Valentina Djakona, Marina Celika, Ieva Nicgala AI DEPENDENCY IN HIGHER EDUCATION: ARE STUDENTS BECOMING OVER-RELIANT?	195-202
Daniela Mirtcheva-Ivanova, Rosen Iliev GENERALIZED NET MODEL OF THE E-LEARNING PROCESS	203-207
Nikolay Nikolov, Georgi Stanchev, Boryana Ilieva – Mihaylova INTELLIGENT INFORMATION SYSTEM FOR TECHNICAL SUPERVISION OF HIGH-RISK FACILITIES	209-214
Dimitar Nikolov WHY DID THREAT ACTORS REPLACE POSHC2 WITH SLIVERC2? COMPARISON OF TWO GREAT C2 FRAMEWORKS	215-218
Dimitar Nikolov DCSYNC ATTACK FROM AN ADVERSARY POINT OF VIEW	219-222
Nikolay Nikolov, Iliyan Vasilev A MULTILAYER FRAMEWORK FOR URBAN MICROCLIMATE ANALYSIS IN SMART SUSTAINABLE CITY DESIGN: THE VIENNA CASE	223-230
Silvia Nikolova, Daniel Denev A SCALABLE RELIABILITY ESTIMATION ALGORITHM FOR COMPLEX COMPUTER NETWORKS UNDER DYNAMIC CONDITIONS WITH AI-BASED EXTENSIONS	231-238
Ventsislava Nikolova-Minkova ARTIFICIAL INTELLIGENCE AND RENEWABLE ENERGY: BIBLIOMETRIC ANALYSIS	239-247
Ihor Panasenko, Kirill Smelyakov, Anastasiya Chupryna, Paulius Sakalys, Loreta Savulioniene Dainius Savulionis COMPARATIVE ANALYSIS OF DEEP LEARNING ARCHITECTURES FOR MONOCHROMATIC IMAGE COLORIZATION	249-255
Trayana Petrova, Panayot Gindev, Iliyana Kamburova UNIVERSITY LIBRARIES IN THE DIGITAL ECOSYSTEM OF CULTURAL MEMORY AND STRATEGIES FOR DIGITIZATION, ACCESS, AND KNOWLEDGE SHARING	257-261
Venelin Rashkov, Alexander Kolev GROUND OPERATIONAL PICTURE IMPROVEMENT THROUGH DIRECT GEOREFERENCING FROM AN UNMANNED AERIAL SYSTEM	263-268
Nataliia Saienko, Zhanna Bogdan, Stanislav Larionov, Tetiana Solodovnyk, Olena Romanovska MULTIMODAL APPROACH TO TEACHING ENGLISH AS A FACTOR IN IMPROVING ENGINEERING STUDENTS' RESEARCH SKILLS	269-277
Elena Shtereva METHODS FOR DATA ARCHIVING AND RECOVERY USING ARTIFICIAL INTELLIGENCE	279-283

Vasil Slavyanov AUTOMATED VULNERABILITY ASSESSMENT IN WINDOWS ACTIVE DIRECTORY AND ORACLE DATABASE ENVIRONMENTS USING POWERSHELL AND SQL*PLUS	285-289
Krasimir Slavyanov COMPUTER VISION APPROACH FOR PANORAMA CREATION IN MILITARY OBSERVATION	291-296
Krasimir Slavyanov A COMPUTER VISION APPROACH TO MILITARY OBJECT RECOGNITION	297-302
Krasimir Slavyanov, Angela Borisova DESIGNING A FIREWALL SYSTEM FOR A COMPUTER NETWORK BASED ON A SINGLE-BOARD COMPUTER	303-308
Georgi Stanchev TURBO ENCODERS WITH HYBRID CONCATENATED CONVOLUTIONAL DESIGN AND TURBO DECODERS WITH SOFT INPUT–SOFT OUTPUT DESIGN IN UNMANNED AERIAL SYSTEMS	309-315
Dimitrina Stefanova, Kristiana Bacheva, Valentin Vasilev PUBLIC TRUST AS A BRIDGE BETWEEN TECHNOLOGY, SOCIETY, AND SUSTAINABILITY	317-323
Ivaylo Stoyanov, Gergana Dimcheva A SURVEY ON CYBERBULLYING IN SMALL AND MEDIUM-SIZED HI-TECH ENTERPRISES IN THE REPUBLIC OF BULGARIA	325-331
Zhaneta Tsoneva THE ROLE OF ARTIFICIAL INTELLIGENCE IN EDUCATIONAL TECHNOLOGIES FOR THE PURPOSES OF HIGHER EDUCATION – EXPERIMENTAL RESEARCH	333-340
Desislava Velinova APPLICATION OF FUZZY LOGIC IN THE PREDICTION OF AIR POLLUTION IN BERLIN, GERMANY	341-347
Martin Zahariev, Daniela Pavlova, Panayot Gindev, George Dimitrov, Vyara Savova, Radoslava Makshutova EMPIRICAL STUDY OF INCIDENT RESPONSE PRACTICES FOR PERSONAL DATA BREACHES IN BULGARIAN ORGANIZATIONS	349-354

Sustainable Energy Engineering and Applications

Ivan Byanov, Nevena Byanova ENERGY COST PRESSURE, AGRICULTURAL INPUT PRICES AND FARM ECONOMIC RESILIENCE IN SELECTED MARKET FARM TYPES: COMPARATIVE EVIDENCE FROM BULGARIA AND THE EU-27	357-362
Olga Borisova BULGARIA’S HYBRID ENERGY MODEL: LEGAL ASPECTS OF SYSTEMIC SUSTAINABILITY	363-369

Olga Borisova	371-377
LEGAL TRANSFORMATION OF THE BULGARIAN ENERGY SECTOR: FROM A CENTRALIZED MODEL TO A DECENTRALIZED REGULATORY FRAMEWORK FOR RENEWABLE ENERGY SOURCES AND RENEWABLE ENERGY COMMUNITIES	
Iliyan Hutov, Petia Nedyalkova, Hristo Hristov	379-386
SECURE AND RESILIENT OPERATION OF HYBRID PV-WIND-STORAGE SYSTEMS FOR MODULAR E-FUEL PRODUCTION UNDER DISTURBANCES	
Misho Matsankov	387-391
ANALYSIS OF MODELS FOR ESTIMATING ELECTRICITY LOSSES IN DISTRIBUTION NETWORKS	
Ventsislava Nikolova-Minkova	393-401
NEGATIVE IMPACT OF RENEWABLE ENERGY: CRITICAL ANALYSIS	
Aadu Petrov, Jaak Jõgi, Külli Hovi, Andres Annuk, Olga Panova, Mart Hovi	403-407
CAPACITY AND SECOND-LIFE POTENTIAL OF LITHIUM-ION CELLS RECOVERED FROM DISPOSABLE E-CIGARETTES FOR DISTRIBUTED MICRO-ENERGY STORAGE	
Atanasi Tashev, Evgeni Dimitrov	409-415
COMPARATIVE ANALYSIS OF EFFICIENCY AND ECONOMIC PERFORMANCE OF A DUAL-FUEL DIESEL ENGINE FUELED WITH COMPRESSED NATURAL GAS AND HYDROGEN	

III

INFORMATION TECHNOLOGY

An Approach for Preventing Overload of the EC2 Service

Evgeni Andreev

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
e.andreev@naval-acad.bg

Desislava Valcheva

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
d.valcheva@naval-acad.bg

Abstract— The aim of this article is to present an approach for preventing service overload in Elastic Compute Cloud (EC2) within Amazon Web Services (AWS). The study analyzes methods for preventing overload of virtual machines in AWS EC2 by comparing vertical and horizontal scaling. Developed block diagrams are presented to visually illustrate the architecture and processes involved in dynamic resource management. A practical implementation of horizontal scaling of virtual machines is also provided. For this purpose, a Python script using the boto3 library has been developed, which fully automates the configuration of key cloud components such as Launch Template, Auto Scaling Group, and Scaling Policy. The proposed solution minimizes the need for manual intervention, protects cloud-based systems from failures during peak loads, and ensures the development of a resilient, flexible, and cost-effective infrastructure. Compared to the manual configuration through the AWS console, the proposed approach groups all required steps into a single Boto3 script that creates the Launch Template, the Auto Scaling Group and the Scaling Policy in one run. The block diagrams visualise both scaling workflows in a unified form, and the scripted procedure can be executed on a schedule through cron, which makes the solution suitable for use in the training of cadets and students at the Nikola Vaptsarov Naval Academy.

Keywords— *Auto Scaling, Boto3 library, Cloud technologies, Virtual machines.*

I. INTRODUCTION

Cloud technologies offer flexible solutions based on the “on-demand service” principle and are widely adopted thanks to their efficiency, scalability, and high availability [1], [2], [3]. Among the main advantages of cloud services are the low initial investment, high availability, and easy scalability of resources. Cloud services enable rapid deployment, offer flexible pricing based on actual usage, ensure greater reliability through automatic updates and recovery from failures, and provide for shared responsibility regarding security between the user and the provider [1], [2], [4], [5].

The use of AWS for creating virtual machines (instances) makes it possible to operate a variety of operating systems that support the processing and storage of data [6], [7]. Through these virtual machines, different types of services can be launched for use either in a local environment or across the public Internet. The virtualization services available in AWS can be automatically scaled both vertically and horizontally, which is of fundamental importance for the design of modern network architectures that require specific analysis of the data exchange protocols [8].

The present article extends the already published AWS configuration procedures in three directions. First, vertical and horizontal scaling in EC2 are compared and described through original block diagrams (Figs. 4 to 6), which summarize the configuration workflow in a form that is not available in this consolidated form in the official documentation. Second, a Boto3 script is developed which performs the creation of the Launch Template, the Auto Scaling Group and a CPU-based Scaling Policy in a single execution, replacing the multi-step procedure that has to be carried out manually through the AWS console as described in [7]. Third, automation will be included in practical training for cadets and students at the Nikola Vaptsarov Naval Academy, in which the script will be executed on a schedule and used as a training configuration, not as a one-time configuration task.

II. MATERIALS AND METHODS

In this work, both horizontal and vertical scaling approaches for active instances are applied. Their use requires the creation of virtual images of pre-installed and pre-configured AWS services - EC2, Auto Scaling and Launch Templates [7]. For access to a Linux-based instance, the secure Secure Shell Protocol (SSH) is used together with the PuTTY client application. To add additional protection (a password) to the private key, PuTTYgen is applied.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.118>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

The automatic creation of virtual machines for preventing system overload and failure through automation of the Auto Scaling service is implemented in the Python programming language using the Boto3 library [7].

III. RESULTS AND DISCUSSION

A. Building a virtual image and accessing a Linux machine

Creating a virtual machine image involves seven steps, as shown in Fig. 1:

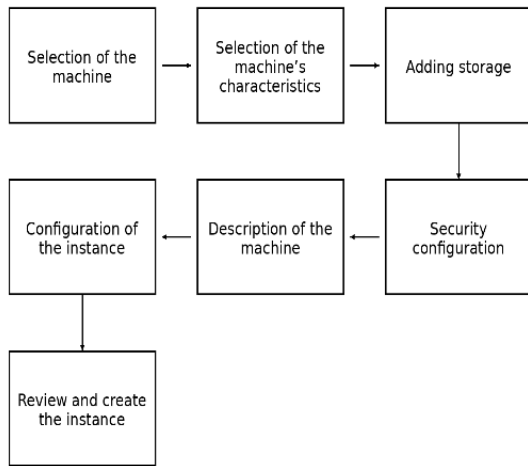


Fig. 1. Sequence for creating a virtual machine image.

One of the key steps in creating an instance is the generation of a cryptographic key pair — public and private — which ensures secure remote access through protocols such as SSH and Remote Desktop Protocol (RDP) [3], [6]. The public key is generated and stored on the AWS side and may be associated with one or more instances, whereas the private key is downloaded only once by the user and remains under their control. Access to the instance can be performed only by the user holding the corresponding private key.

The private key may be in Privacy Enhanced Mail (PEM) or PuTTY Private Key (PPK) format. The PPK format is used directly for SSH access through software such as PuTTY, while the PEM format is used with Windows-based instances to decrypt the initial administrator password. After successful use in the AWS “Password recovery” service and entering the private key, the username and password for accessing the virtual machine are displayed. The PEM and PPK formats can be converted to add additional protection through a passphrase, which raises the level of security [3], [9]. This functionality is implemented through the PuTTYgen tool. Access to virtual machines is granted only when both a valid private key and the corresponding passphrase, if configured, are provided.



Fig. 2. Linux instance created in AWS with the main instance details shown.

Fig. 2 shows access to a Linux-based instance, which is performed via the SSH protocol using a client application such as PuTTY. When the remote connection between the client and the virtual machine is established, a private key is presented and is validated against the corresponding public key associated with the instance; when the keys match, administrative access is granted. After the session is established, the user can manage the operating system. Before installing additional services or configurations, it is recommended to update the operating system using the command: “sudo yum update -y”. Fig. 3 presents the result of executing the command sudo yum update -y.

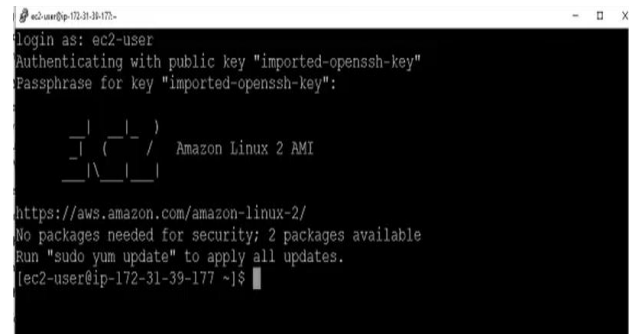


Fig. 3. Running Linux instance with the distribution updated.

B. Building and accessing a virtual image of a Windows Server 2025 machine

Creating a Windows Server 2025 instance is analogous to creating a Linux-based instance (Fig. 3); the main difference is the protocol used for remote access — RDP [3].

Different software tools may be used for remote management of the instance, regardless of the client operating system in use (Windows / Windows Server, Linux-based systems, or macOS). For example, with Windows-based virtual images the Remote Desktop Connection application included with the Windows operating system is used by default.

C. Scalability of cloud systems through horizontal and vertical scaling

a) Vertical scaling approach

In vertical scaling, a single instance, or a limited number of instances, is used; instead of adding or removing instances, the computing resources of the existing ones (CPU, RAM, etc.) are increased. This approach typically involves higher costs, as larger resource configurations are paid for regardless of the current load. In practice, situations are often observed in

which the available resources are insufficient under high instance load, or, conversely, a significant share of them remain unused at low request intensity, which leads to inefficiency from an economic point of view. Increasing resources usually requires temporarily stopping the instance, which causes a brief service interruption. In addition, decreasing resources after they have been increased is often limited or even impossible in certain configurations. Although this approach provides scalability, it is characterized by greater complexity and higher costs; nevertheless, it remains the preferred option in several scenarios [6], [10].

b) Horizontal scaling approach

Another AWS service used for automatic scaling is Auto Scaling. It relies on a previously prepared template for creating virtual machines. The basic requirements for creating new virtual machines are the template name, and the choice of initial cloud computing resources such as CPU cores, RAM, and Internet connection bandwidth. Further requirements for creating the template include defining scalability parameters based on increasing or decreasing the average load of the virtual CPU cores. For example, the following criterion may be selected: if the average load exceeds 60%, a new virtual machine is to be created. The new instance can reduce the load on a previously created virtual machine by distributing the load between the two machines through the load-balancing service, which is also provided by AWS. Other criteria for creating new machines may include high inbound or outbound network traffic, and others [11].

The approach of preventing service failure through automation of Auto Scaling is referred to as horizontal because it allows multiple virtual machines to be created in order to compensate for the load [7], [12]. These machines have identical baseline settings in terms of computing power, based on the previously created template. For this functionality to operate correctly, three values are defined in the template:

- Minimum number of machines required by the customer to be running.
- Desired number of machines to be running when the service is first activated.
- Maximum number of machines to be running under peak load.

In this way, the service administrator can decide how many machines should run as the minimum, calculate the financial resources to be allocated, and determine the maximum number of machines accordingly. A larger number of machines than the chosen maximum cannot be created automatically. The advantages of this type of automatic horizontal scaling can be illustrated by the following example: if a user of the AWS service selects a desired count of two machines, a minimum of one and a maximum of three, then two machines will be created based on the prepared template. If, however, there is insufficient load on them, the count will be automatically reduced to one. If the load exceeds the values defined in

the template, new machines will be created automatically up to the selected maximum threshold. For automating scaling, the horizontal approach is more appropriate than the vertical one, because the load is distributed across many machines with smaller computing capabilities.

Creating a launch template for instances:

Fig. 4 visualizes the process of creating a single, uniformly configured virtual machine with specific parameters, which is subsequently used as a template for launching identical machines.

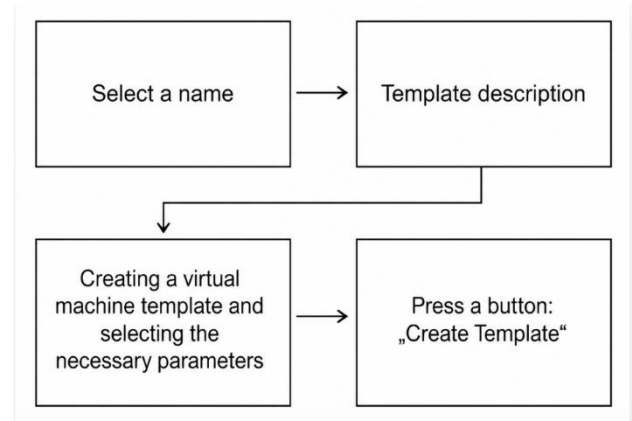


Fig. 4. The process of creating a template with parameters chosen by the user.

Creating a launch template for identical instances is part of configuring the automatic scaling service.

Configuring the Auto Scaling service

Configuring the automatic scaling service involves seven steps, as shown in Fig. 5:

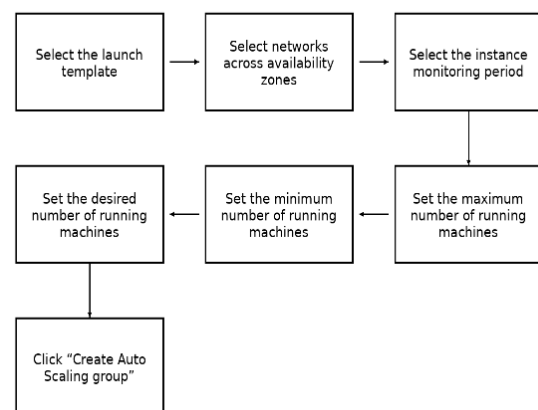


Fig. 5. The process of configuring automatic scaling of machines.

This procedure for configuring the automatic scaling service takes more time than using Software Development Kit (SDK) code in AWS. In this paper, a solution to the scaling automation task is proposed using the Python programming language and the Boto3 library.

D. An approach to automating Auto Scaling Group using the Boto3 library

Automating the Auto Scaling Group using the boto3 library enables interaction with AWS services. Examples of applications of Boto3 include the creation of virtual machines, storage, automatic creation of virtual machines, and others [7], [10].

The block diagram visualized in Fig. 6 shows the steps for creating a script that automates the Auto Scaling Group.

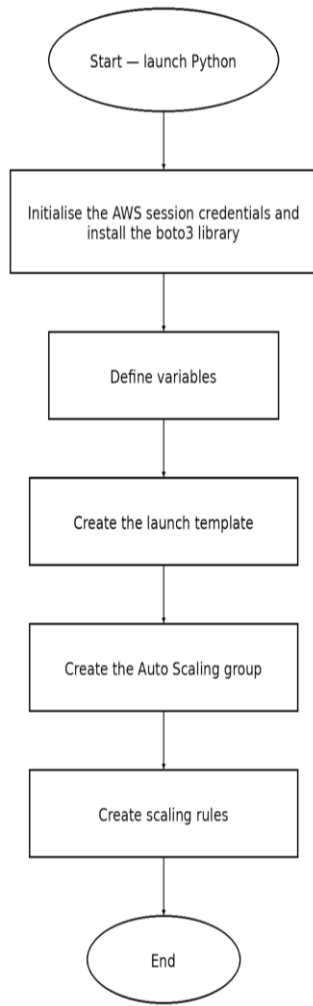


Fig. 6. Steps for creating a script that automates the Auto Scaling Group.

The script automates the creation of a Launch Template, an Auto Scaling Group and a Scaling Policy in AWS through the boto3 library. At the start, clients are initialized for EC2 and Auto Scaling. Next, the basic parameters are defined (AMI ID, instance type, key, zones, etc.). An EC2 Launch Template is created and is used to launch instances. After that, an Auto Scaling Group is created with a minimum and a maximum number of instances. Finally, an automatic scaling policy is added that increases the number of instances on demand. An example of such automation is shown in Fig. 7.

Fig. 7 presents the code of a script for creating a Launch Template and an Auto Scaling Group in AWS with automatic scaling at 50% CPU utilisation of the machines. Including a cron job [13] for executing the script on a schedule will improve the efficiency of repetitive tasks in AWS.

The presented methods for EC2 automation - with a graphical interface and using a Python script, will be used to create an automated training system for cadets and students at the Nikola Vaptsarov Naval Academy.

```

import boto3

REGION = "eu-central-1"
VPC_ID = "vpc-xxxxxxx"

ec2 = boto3.client("ec2", region_name=REGION)
asg = boto3.client("autoscaling", region_name=REGION)
ssm = boto3.client("ssm", region_name=REGION)

ami = ssm.get_parameter(
    Name="/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64"
)["Parameter"]["Value"]

subs = [
    {
        "SubnetId":
            for s in ec2.describe_subnets(
                Filters=[{"Name": "vpc-id", "Values": [VPC_ID]}]
            )["Subnets"][:3]
    }
]

lt = ec2.create_launch_template(
    LaunchTemplateName="demo-lt",
    LaunchTemplateData={
        "ImageId": ami,
        "InstanceType": "t3.micro",
    },
)["LaunchTemplate"]

asg.create_auto_scaling_group(
    AutoScalingGroupName="demo-asg",
    MinSize=1,
    DesiredCapacity=2,
    MaxSize=3,
    VPCZoneIdentifier=".".join(subs),
    LaunchTemplate={
        "LaunchTemplateId": lt["LaunchTemplateId"],
        "Version": str(lt["LatestVersionNumber"]),
    },
)

asg.put_scaling_policy(
    AutoScalingGroupName="demo-asg",
    PolicyName="cpu50",
    PolicyType="TargetTrackingScaling",
    TargetTrackingConfiguration={
        "PredefinedMetricSpecification": {
            "PredefinedMetricType": "ASGAverageCPUUtilization"
        },
        "TargetValue": 50.0,
    },
)

print("DONE")
    
```

Fig. 7. Python (boto3) script for creating a Launch Template and an Auto Scaling Group.

CONCLUSIONS

The analysis carried out in the present paper shows that vertical scaling allows the computing resources of existing instances to be increased, but it is associated with higher costs, limited flexibility, and the need for a temporary service interruption. Horizontal scaling, in turn, implemented through Auto Scaling, ensures better resilience and effective distribution of the resource load through the dynamic addition and removal of virtual machines according to current needs.

The presented automation approach using the boto3 library and the Python programming language demonstrates the possibilities for building a flexible and adaptive cloud infrastructure. By defining a Launch Template, an Auto Scaling Group and Scaling policies, automatic resource management is achieved, which minimizes the risk of instance overload and failure. The use of automated mechanisms, including the execution of tasks through a cron job, additionally improves efficiency and reduces the need for manual intervention.

The contribution of the present work is the unification of the Launch Template, an Auto Scaling Group and a Scaling Policy into a single Boto3 script with the goal of using this script within a training environment for cadets and students. Further work is planned in two directions. The first one is to extend the automation with load testing based on different scaling policies. The second one is to introduce indicators for the learning outcomes when the script is applied as a laboratory exercise.

In conclusion, combining horizontal and vertical scaling, together with the automation of processes, represents an effective strategy for building reliable, scalable, and economically optimised cloud systems that meet today's requirements for the high availability and performance of virtual machines.

REFERENCES

- [1] T. Erl, R. Puttini, and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*. Upper Saddle River, NJ, USA: Prentice Hall, 2014. ISBN: 978-0133387520.
- [2] S. Cambric and M. T. Ratemo, *Cloud Auditing Best Practices: Perform Security and IT Audits across AWS, Azure, and GCP by Building Effective Cloud Auditing Plans*. Birmingham, UK: Packt Publishing, 2023. ISBN: 978-1803243771.
- [3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, NIST Special Publication 800-145, 2011. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [Accessed: Apr. 25, 2026], <https://doi.org/10.6028/NIST.SP.800-145>.
- [4] D. Carter, *CCSP Certified Cloud Security Professional All-in-One Exam Guide*, 3rd ed. New York, NY, USA: McGraw-Hill, 2022. ISBN: 978-1264842209.
- [5] C. Bravo and D. Kitchen, *Mastering Defensive Security: Effective Techniques to Secure Your Windows, Linux, IoT, and Cloud Infrastructure*. Birmingham, UK: Packt Publishing, 2021. ISBN: 978-1800208162.
- [6] C. Dotson, *Practical Cloud Security: A Guide for Secure Design and Deployment*. Sebastopol, CA, USA: O'Reilly Media, 2019. ISBN: 978-1492037514.
- [7] Amazon Web Services, "AWS Documentation." [Online]. Available: <https://docs.aws.amazon.com/> [Accessed: Apr. 25, 2026].
- [8] D. Dimitrova, "An analytical model for multi-criteria evaluation of IoT application layer protocols," in *Proc. 8th Int. Symp. Innovative Approaches in Smart Technologies (ISAS)*, Istanbul, Turkey, 2024. IEEE. ISBN: 9798331540104, <https://doi.org/10.1109/ISAS64331.2024.10845381>.
- [9] D. Dimitrova, "Evaluating the effectiveness of practical exercises in cryptography and authentication courses of cybersecurity education," *Mathematics and Education in Mathematics*, vol. 54, pp. 118–124, 2025, <https://doi.org/10.55630/MEM.2025.54.118-124>.
- [10] R. Buyya, C. Vecchiola, and S. T. Selvi, *Mastering Cloud Computing*. New York, NY, USA: McGraw-Hill Education, 2013.
- [11] D. Dimitrova, "Selection and justification of criteria for comparative analysis of lightweight ciphers," *Mathematics and Informatics*, vol. 66, no. 5, pp. 534–542, 2023, <https://doi.org/10.53656/math2023-5-8-sel>.
- [12] "What is Amazon EC2 Auto Scaling?" [Online]. Available: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html> [Accessed: Apr. 25, 2026].
- [13] "Cron-job.org." [Online]. Available: <https://cron-job.org/en/> [Accessed: Apr. 25, 2026].

On Some Properties of Posterior Predictive Distributions

Ralitsa Angelova-Slavova

Department of Communication and Information Systems
 "Vasil Levski" National Military University
 Veliko Tarnovo, Bulgaria
 rslavova@nvu.bg

Dimitar Tsvetkov

Department of Communication and Information Systems
 "Vasil Levski" National Military University
 Veliko Tarnovo, Bulgaria
 dptsvetkov@nvu.bg

Abstract – This article considers the method of posterior predictive distributions as the one of the specific tools for checking the correspondence between data and the statistical model. The generated examples demonstrate that in the role of posterior predictive testing statistics (as a discrepancy measure), dispersion measures should be taken, because the central tendency measures do not give the expected results.

Keywords – Posterior predictive distributions, Markov chain Monte Carlo (MCMC), Metropolis–Hastings algorithm, Data fitting methods.

I. INTRODUCTION

Let a random sample $x_{(j)} \sim f(x|\theta)$ with a size J be given from some distribution $f(x|\theta)$. The estimation for the parameters θ can be performed using the Bayesian method, which examines the posterior distribution of θ , given prior distribution $f(\theta) = f(\theta|\tau)$ with some known hyper-parameters τ [1], [2], [3] and [4]. The likelihood function has the form

$$f(\mathbf{x}|\theta) = \prod_j f(x_{(j)}|\theta)$$

and $f(\mathbf{x}|\theta)f(\theta)$ is the joint distribution of the data $\mathbf{x} = (x_{(j)})$ and the parameters θ . For the posterior distribution of θ we have

$$f(\theta|\mathbf{x}) \propto f(\mathbf{x}|\theta)f(\theta) = \left(\prod_j f(x_{(j)}|\theta) \right) f(\theta)$$

In this paper, by $f(\cdot)$ we will denote densities of given distributions, which will distinguish through the structure of the arguments.

II. MATERIALS AND METHODS

This paper brings more theoretical content, which requires using of proper software. Here we use a specific Markov chain Monte Carlo (MCMC) technique, known as

Metropolis – Hastings algorithm. Where necessary, numbers are rounded to the third digit after the decimal point. The form of $f(\theta|\mathbf{x})$ usually is not easy to find. Its relief however can be achieved by mentioned MCMC method after generating a sufficient number of observations [5], [6], [7] and [8]. The popular Metropolis – Hastings algorithm with independent choice offers the following option. For the working distribution $q(\theta|\theta')$ we set the prior $f(\theta)$ and the target distribution $\pi(\theta)$ is of course the posterior one

$$\pi(\theta) = f(\theta|\mathbf{x}) \propto \left(\prod_j f(x_{(j)}|\theta) \right) f(\theta)$$

The algorithm scheme looks like this. Start by choosing an initial observation $\theta_{(0)}$. Then for a known $\theta_{(n-1)}$ do the following.

1. Select a candidate $\theta_* \sim f(\theta)$ and calculate

$$\alpha = \min \left(1, \frac{\prod_j f(x_{(j)}|\theta_*)}{\prod_j f(x_{(j)}|\theta_{(n-1)})} \right)$$

2. Generate $u \sim U(0,1)$. If $0 < u < \alpha$ the candidate is accepted and put $\theta_{(n)} = \theta_*$. Otherwise the candidate is rejected and put $\theta_{(n)} = \theta_{(n-1)}$.

In this way we obtain a random sample of observations $(\theta_{(n)})$ from the posterior distribution $f(\theta|\mathbf{x})$. Their local dependence can be mitigated by including in the sample only the members with index $n = ki$, for some fixed $k \in \mathbb{N}$ [9].

Example 1. Let $x_{(j)} \sim \text{Poisson}(\lambda)$ be a random sample with size J from a Poisson distribution with parameter $\lambda > 0$. Then

$$f(\mathbf{x}|\lambda) = \prod_{j=1}^J e^{-\lambda} \frac{\lambda^{x_{(j)}}}{x_{(j)}!} \propto e^{-J\lambda} \lambda^{J\bar{x}}$$

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.37>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

About the parameter λ we assume a gamma prior distribution $\lambda \sim \text{Gamma}(\alpha, \beta)$, where α (shape) and β (rate) are beforehand chosen hyper-parameters. For the joint density of $\mathbf{x}$ and λ we have

$$f(\mathbf{x}, \lambda) = \left(\prod_{j=1}^J e^{-\lambda} \frac{\lambda^{x_{(j)}}}{x_{(j)}!} \right) \frac{\beta^\alpha \lambda^{\alpha-1} e^{-\lambda\beta}}{\Gamma(\alpha)}$$

A random sample of size $J = 100$ was taken from $\text{Poisson}(3)$ distribution. The M-H algorithm here is specified as follows. Assume $\alpha = \bar{x}$ and $\beta = 1$, for which the mean of the prior distribution coincides with the mean of the data. Choose $\lambda_{(0)} \sim \text{Gamma}(\bar{x}, 1)$. Let the observation $\lambda_{(n-1)}$ be known. Then for the next observation $\lambda_{(n)}$ do the following.

1. Select a candidate $\lambda_* \sim \text{Gamma}(\bar{x}, 1)$ and calculate

$$a = \min \left(1, \frac{e^{-J\lambda_*} \lambda_*^{J\bar{x}}}{e^{-J\lambda_{(n-1)}} \lambda_{(n-1)}^{J\bar{x}}} \right)$$

2. Generate $u \sim U(0,1)$. If $0 < u < a$ the candidate is accepted and put $\lambda_{(n)} = \lambda_*$. Otherwise the candidate is rejected and put $\lambda_{(n)} = \lambda_{(n-1)}$.

Perform $m = 1\,000$ initial iterations and yet $N = 1\,000\,000$ basic iterations, from which we take every 100-th in a row [9], obtaining a random sample of size 10 000. On the other hand

$$f(\mathbf{x}, \lambda) \propto e^{-(\beta+J)\lambda} \lambda^{(\alpha+x_{(1)}+\dots+x_{(J)})-1}$$

whence the posterior distribution $f(\lambda|\mathbf{x})$ appears as the following gamma distribution

$$\text{Gamma}(\alpha + x_{(1)} + \dots + x_{(J)}, \beta + J)$$

Fig. 1 shows a very good practical fit between the histogram of the MCMC sample and the corresponding theoretical gamma distribution [$\text{ChiSquare}(9) = 7.582; p\text{-value} = 0.577$]. The following Table 1 contains sample estimated characteristics of the posterior distribution $f(\lambda|\mathbf{x})$, including the hyper-parameters *shape* and *rate*.

TABLE 1. COMPARISON BETWEEN VALUES.

	Shape	Rate	Mean	SD
Theoretical	312.090	101	3.090	0.175
Empirical	315.793	102.247	3.089	0.174

III. RESULTS AND DISCUSSION

Let data observations $\mathbf{x}_{obs} = (o_{(j)})$ be given, for which a statistical model with a likelihood function $f(\mathbf{x}|\theta)$ is assumed with certain parameters θ . Posterior predictive distributions are formed by generating new possible data $\mathbf{x}_{rep}$, according to the observed data $\mathbf{x}_{obs}$ [10], [11] and [12]. This new possible data is generated by means of the formula

$$\mathbf{x}_{rep(n)} \sim f(\mathbf{x}|\mathbf{x}_{obs}) = \int f(\mathbf{x}|\theta) f(\theta|\mathbf{x}_{obs}) d\theta$$

where $f(\theta|\mathbf{x}_{obs})$ is the posterior distribution of θ . Any observation $\theta_{(n)} \sim f(\theta|\mathbf{x}_{obs})$ gives a response $\mathbf{x}_{rep(n)}$ by random selection $\mathbf{x}_{rep(n)} \sim f(\mathbf{x}|\theta_{(n)})$.

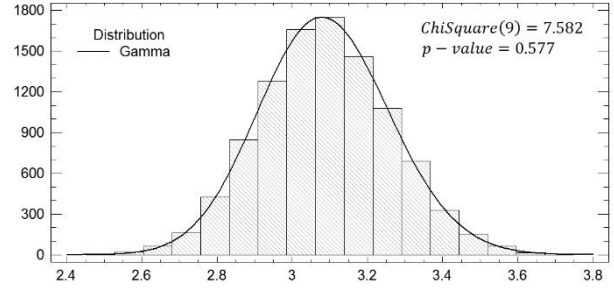


Fig 1. Explanation to Example 1.

Let $g(\mathbf{x})$ be some test statistic for the model $f(\mathbf{x}|\theta)f(\theta)$. Then $(g(\mathbf{x}_{rep(n)}))$ are observations for the random variable $g(\mathbf{x})$. The belonging of the particular value $g(\mathbf{x}_{obs})$ far from the center of the empirical distribution of $(g(\mathbf{x}_{rep(n)}))$ indicates a misfit between the model and the data.

The reader may see [13], [14], [15] and [16], where this approach is rigorously grounded.

Example 2. In Example 1, $\mathbf{x}_{obs}$ are actually generated from $\text{Poisson}(3)$ distribution. Let the test statistic be the standard deviation $\sigma(\mathbf{x})$. We perform 10 000 data generations $(\mathbf{x}_{rep(n)})$, based on the one constructed in Example 1 sample from $f(\lambda|\mathbf{x}_{obs})$. The distribution of standard deviations is presented in the following Fig. 2.

For the observed data, we have $\sigma(\mathbf{x}_{obs}) = 1.787$, which represents approximately the 61% quantile for the empirical posterior predictive distribution of $(\sigma(\mathbf{x}_{rep(n)}))$ observations. This value is close to the center of the distribution and indicates a good enough fit between data and the assumed model, which is an expected result, since the data are actually generated from a Poisson distribution.

Example 3. Go back to Example 1, but this time let data be generated from a uniform distribution between the integers 0 and 9. Again, we will look for a model with a Poisson distribution, and as in Example 2, we will examine the posterior predictive distribution of $\sigma(\mathbf{x}_{rep})$. We repeat the scheme from the previous two examples with 10000 observations $(\mathbf{x}_{rep(n)})$. The empirical distribution of the corresponding standard deviations is shown in Fig. 3.

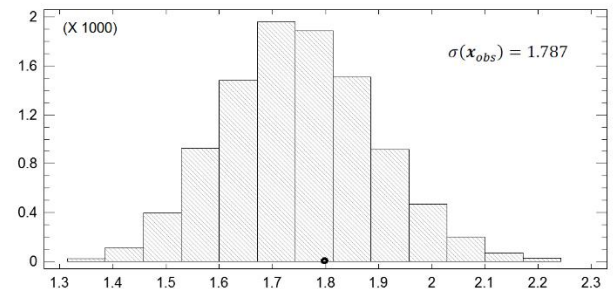


Fig 2. Histogram of $(\sigma(\mathbf{x}_{rep(n)}))$ for Example 2.

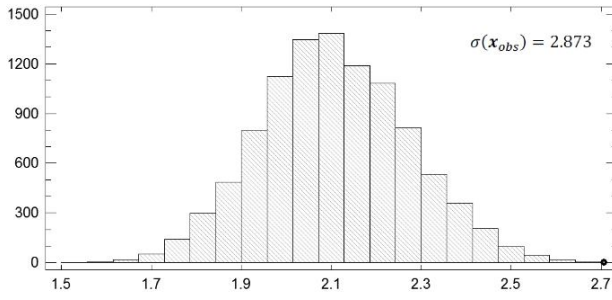


Fig. 3. Histogram of $(\sigma(\mathbf{x}_{rep(n)}))$ for Example 3.

For the observed data, we have $\sigma(\mathbf{x}_{obs}) = 2.873$, which lies far in the right tail of the posterior predictive distribution. This value indicates a poor fit between the observed data and the actually assumed model.

Example 4. Let $x_{(j)} \sim \text{Geometric}(p)$ be a random sample with size J from the (zero based) geometric distribution with parameter $0 < p < 1$. Then

$$\begin{aligned} f(\mathbf{x}|p) &= \prod_{j=1}^J (1-p)^{x_{(j)}} p = p^J (1-p)^{x_{(1)} + \dots + x_{(J)}} \\ &= p^J (1-p)^{J\bar{x}} \end{aligned}$$

The parameter p is assumed to have beta prior distribution $p \sim \text{Beta}(\alpha, \beta)$, where the hyper-parameters α (shape) and β (shape) are chosen in advance. For the joint density of $\mathbf{x}$ and p we have

$$f(\mathbf{x}, p) \propto p^{\alpha+J-1} (1-p)^{\beta+J\bar{x}-1} \sim \text{B}(\alpha+J, \beta+J\bar{x})$$

For this Example 4 is realized a random sample of size $J = 100$ from distribution $\text{Geometric}(0.1)$. The M-H algorithm here is specified as follows. Assume $\alpha = 1$ and $\beta = 1 + \bar{x}$, under which the mean of the prior distribution coincides with the MLE estimate of p from the observed data.

Choose $p_{(0)} \sim \text{Beta}(1, 1 + \bar{x})$ and suppose the observation $p_{(n-1)}$ is known. Then for the next one $p_{(n)}$ do the following.

1. Select a candidate $\lambda_* \sim \text{Gamma}(\bar{x}, 1)$ and calculate

$$\alpha = \min \left(1, \frac{p_*^{\alpha+J-1} (1-p_*)^{\beta+J\bar{x}-1}}{p_{(n-1)}^{\alpha+J-1} (1-p_{(n-1)})^{\beta+J\bar{x}-1}} \right)$$

2. Generate $u \sim U(0,1)$. If $0 < u < \alpha$ the candidate is accepted and set $p_{(n)} = p_*$. Otherwise, the candidate is rejected and set $p_{(n)} = p_{(n-1)}$.

Now perform $m = 1000$ initial iterations and yet more $N = 1\,000\,000$ basic iterations, from which take every 100-th in turn. In this way we get a good random sample from $f(\lambda|\mathbf{x})$ with a size 10 000. The posterior distribution $f(p|\mathbf{x})$ is beta $\text{B}(\alpha+J, \beta+J\bar{x})$.

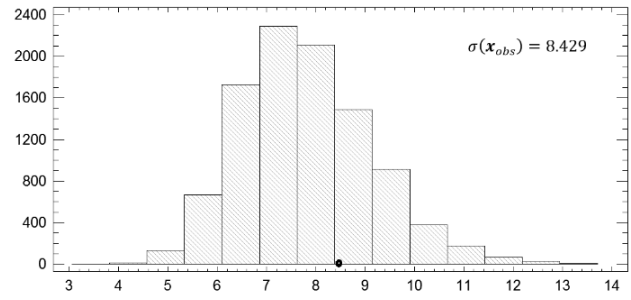


Fig. 4. Histogram of $(\sigma(\mathbf{x}_{rep(n)}))$ for Example 4.

Let, as in Example 2, the test statistic be the standard deviation $\sigma(\mathbf{x})$ and let perform 10 000 data generations. $(\mathbf{x}_{rep(n)})$. The distribution of standard deviations is given in Fig. 4.

For the observed data, we have $\sigma(\mathbf{x}_{obs}) = 8.429$, which represents approximately the 71% quantile for the empirical posterior predictive distribution. This value is close to the center of the distribution and indicates a good fit between the observed data and the model, which is an expected result since the data are actually generated from a geometric distribution.

Example 5. Consider again Example 4, but this time the data is generated from a uniform distribution between the integers 0 to 9. Again, we will look for a model with a geometric distribution, and as in example 4, we will examine the posterior predictive distribution of $\sigma(\mathbf{x}_{rep})$. We repeat the scheme from the previous examples with 10 000 generations $(\mathbf{x}_{rep(n)})$. The following Fig. 5 shows the empirical predictive distribution of the standard deviations.

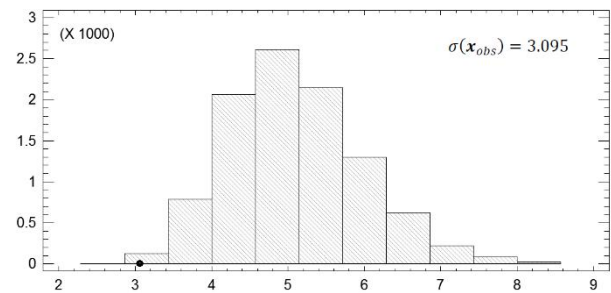


Fig. 5. Histogram of $(\sigma(\mathbf{x}_{rep(n)}))$ for Example 5.

For the observed data, we have $\sigma(\mathbf{x}_{obs}) = 3.095$, which is approximately the 0.15% quantile for the empirical posterior predictive distribution and lies far from the center of the distribution. This fact confirms the misfit between the observed data and the assumed model.

The above examples raise a further discussion about the extent to which the size of the empirical sample affects the results. The question of finding a wider variety of test statistics that highlight the lack of fit between the data and the model also remains under further discussion.

IV. CONCLUSIONS

Posterior predictive distributions provide a unique method for testing the fit between the observed data and the corresponding statistical model. Some measure of dispersion should be chosen as a test statistic, because the measures of central tendency are not sufficiently consistent with the method, described above. More information about this approach, the reader can find for example in [13], [14], [15] and [16].

One may conclude that unimodal distributions are similar in their central areas, and the differences appear in the tails of their distributions.

V. ACKNOWLEDGMENTS

The authors are very grateful to the department colleagues for the support of this work, which was partially developed in the framework with the national project BG05M2OP001-2.016-0003 "Modernization of the National Military University "Vasil Levski" and Sofia University "St. Kliment Ohridski".

REFERENCES

- [1] M. Aitkin, Statistical Inference: An Integrated Bayesian/Likelihood Approach (1st ed.). Chapman and Hall/CRC. <https://doi.org/10.1201/EBK1420093438>
- [2] I. Ntzoufras, Bayesian modeling using WinBUGS, Hoboken, N. J: Wiley, 2009.
- [3] P. Congdon, Bayesian Models for Categorical Data, New York: Wiley, 2005.
- [4] J. Albert, Bayesian Computation with R, 2nd ed., New York: Springer, 2009. <https://doi.org/10.1007/978-0-387-92298-0>
- [5] N. Metropolis, A. Rosenbluth, M. Rosenbluth, A. Teller and E. Teller, "Equations of state calculations by fast computing machines," J. Chem. Phys., vol. 21, pp. 1087-1091, 1953. <https://doi.org/10.1063/1.1699114>
- [6] C. P. Robert and G. Casella, Monte Carlo statistical methods, New York: Springer, 2004.
- [7] C. P. Robert and G. Casella, Introducing Monte Carlo methods with R, New York: Springer, 2010.
- [8] R. Angelova-Slavova, Convergence and Applications of the Metropolis-Hasting algorithm, Plovdiv: Astarta, 2020.
- [9] W. Link and M. Eaton, M. "On thinning of chains in MCMC," Methods in Ecology and Evolution, vol. 3, pp. 112-115, 2012. <https://doi.org/10.1111/j.2041-210X.2011.00131.x>
- [10] A. Gelman, X.-L. Meng and H. Stern, "Posterior Predictive Assessment of Model Fitness via Realized Discrepancies," Statistica Sinica, vol. 6(4), pp. 733-807, 1996. [Online]. Oxford Reference Online, <https://sites.stat.columbia.edu/gelman/research/published/A6n41.pdf>, [Accessed December 06, 2025].
- [11] M. A. Tanner and W. H. Wong, "The Calculation of Posterior Distributions by Data Augmentation," Journal of the American Statistical Association, vol. 82(398), pp. 528-540, 1987.
- [12] M. M. Barbieri and J. O. Berger, "Optimal predictive model selection," Ann. Statist., vol. 32(3), pp. 870-897, 2004. <https://doi.org/10.1214/009053604000000238>
- [13] X.-L. Meng, "Posterior predictive p-values", The Annals of Statistics, vol. 22(3), pp. 1142-1160, 1994.
- [14] T. Ando, Bayesian Model Selection and Statistical Modeling, Taylor and Francis Group, 2010.
- [15] J.-P. Fox, Bayesian Item Response Modeling. Theory and Applications, New-York: Springer, 2010. <https://doi.org/10.1007/978-1-4419-0742-4>
- [16] C. A. Stone and Z. Xiaowen, Bayesian Analysis of Item Response Theory Models Using SAS, Cary, NC: SAS Institute Inc., 2015.

Some Properties of the Dirichlet Type Integrals

Ralitsa Angelova-Slavova

Department of Communication and Information Systems
 "Vasil Levski" National Military University
 Veliko Tarnovo, Bulgaria
 rslavova@nvu.bg

Dimitar Tsvetkov

Department of Communication and Information Systems
 "Vasil Levski" National Military University
 Veliko Tarnovo, Bulgaria
 dptsvetkov@nvu.bg

Abstract – This article considers the Dirichlet type integrals, for which closed form formulas have been obtained. In particular, it is proven that all these integrals are rational numbers. Feynman's method for integral calculating is also used in the work. The integrals considered are related to a remarkable Lobachevsky formula, described at the end.

Keywords – Dirichlet integral, Feynman integration method, Lobachevsky integral formula.

I. INTRODUCTION

Dirichlet integral [1], [2]

$$\mathcal{D} = \int_0^{\infty} \frac{\sin x}{x} dx$$

has a key role in the theory of the Fourier transform [3], [4], [5].

This integral is an important (perhaps the most important) example of a conditionally convergent integral [6]. We have

$$\int_0^{\infty} \left| \frac{\sin x}{x} \right| dx = \infty$$

because

$$\int_0^{n\pi} \left| \frac{\sin x}{x} \right| dx \geq \frac{2}{\pi} \sum_{k=1}^n \frac{1}{k} \approx \frac{2}{\pi} \ln n \rightarrow \infty$$

Any interesting property of this integral is supposed to be the subject of special attention with a presumed eventual application in signal processing theory.

II. MATERIALS AND METHODS

This paper offers mainly theoretical content. The results are additionally verified empirically by examining many particular cases using specialized software for analytic transformations. Feynman's famous (brilliant) method for calculating some parametric integrals is also used here [7], [8], which offers an original way to estimate

$\mathcal{D}$. Also, in the text below various calculus technics are used, including the classic Laplace Transform.

The value of $\mathcal{D}$ is $\pi/2$, which can be shown in various ways, one of which is related to the Feynman approach. Put

$$J(a) = \int_0^{\infty} \frac{\sin x}{x} e^{-ax} dx$$

where $a \geq 0$ is a parameter. Then we have

$$\begin{aligned} J'(a) &= \int_0^{\infty} \frac{\sin x}{x} e^{-ax} (-x) dx \\ &= - \int_0^{\infty} \sin x e^{-ax} dx = - \frac{1}{1+a^2} \end{aligned}$$

from which we find

$$J(a) = - \int \frac{da}{1+a^2} + const = - \arctan a + const$$

On the other hand, $J(\infty) = 0$, therefore

$$0 = - \arctan \infty + const$$

$$0 = - \frac{\pi}{2} + const \Rightarrow const = \frac{\pi}{2}$$

which gives

$$J(a) = - \arctan a + \frac{\pi}{2}$$

$$\mathcal{D} = J(0) = \arctan 0 + \frac{\pi}{2} = \frac{\pi}{2}$$

III. RESULTS AND DISCUSSION

The main result of this article is contained in the following theorem.

Theorem 1. Consider the Dirichlet type integrals

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.38>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#)

$$\mathcal{D}_n = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^n dx, n \in \mathbb{N}$$

1) Let $n = 2m + 1$, $m \in \mathbb{N}$, be an odd number. Put $z_k = -(2k + 1)^2$, $0 \leq k \leq m$,

$$f(z) = (z - z_0)(z - z_1) \cdots (z - z_m)$$

Then

$$\mathcal{D}_n = \frac{n}{2} \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \frac{1}{(2k + 1)}$$

2) Let $n = 2m$, $m \in \mathbb{N}$, be an even number. Put $z_k = -(2k)^2$, $1 \leq k \leq m$,

$$f(z) = (z - z_1)(z - z_2) \cdots (z - z_m)$$

Then

$$\mathcal{D}_n = \frac{n}{4} \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \frac{1}{k}$$

3) For every natural number $n \in \mathbb{N}$, the value of the integral $\mathcal{D}_n$ is a rational number.

We will give the proof of Theorem 1 right below. In particular

$$\mathcal{D}_1 = \frac{1}{\pi} \int_0^\infty \frac{\sin x}{x} dx = \frac{1}{2}, \mathcal{D}_2 = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^2 dx = \frac{1}{2}$$

$$\mathcal{D}_3 = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^3 dx = \frac{3}{8}$$

$$\mathcal{D}_4 = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^4 dx = \frac{1}{3}$$

$$\mathcal{D}_{10} = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^{10} dx = \frac{15619}{72576}$$

$$\mathcal{D}_{20} = \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^{20} dx = \frac{37307713155613}{243290200817664}$$

$$\begin{aligned} \mathcal{D}_{30} &= \frac{1}{\pi} \int_0^\infty \left(\frac{\sin x}{x} \right)^{30} dx \\ &= \frac{18497593486903125823791655511}{147362699895661699242393600000} \end{aligned}$$

All $\mathcal{D}_n$ are absolutely convergent for $n \geq 2$.

PROOF OF THEOREM 1. Hereafter $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{R}$ are the traditional notations for the natural, the rational and the real numbers respectively. Start with a proposition, the validity of which follows from the properties of the Laplace transform.

Proposition 1. For every natural number $n \in \mathbb{N}$ it holds

$$\int_0^\infty s^{n-1} e^{-sx} ds = \frac{\Gamma(n)}{x^n} = \frac{(n-1)!}{x^n}, x > 0$$

where $\Gamma(\cdot)$ is the Euler gamma function. ■

Proposition 1 allows to represent the integrals $\mathcal{D}_n$ in the form

$$\mathcal{D}_n = \frac{1}{\pi(n-1)!} \int_0^\infty \sin^n x \left(\int_0^\infty s^{n-1} e^{-sx} ds \right) dx$$

After changing the order of integration, we obtain

$$\mathcal{D}_n = \frac{1}{\pi(n-1)!} \int_0^\infty s^{n-1} \left(\int_0^\infty \sin^n x e^{-sx} dx \right) ds \quad (1)$$

The validity of the following proposition is a consequence from the representation of a proper rational function as a sum of elementary fractions.

Proposition 2. Let $Q(z)$ be a polynomial with $\deg Q \leq m-1$, $m \in \mathbb{N}$, and $z_k \in \mathbb{C}$, $1 \leq k \leq m$, are distinct numbers. Let also

$$f(z) = (z - z_1) \cdots (z - z_m)$$

Then

$$\frac{Q(z)}{f(z)} = \sum_{k=1}^m \frac{a_k}{z - z_k}, a_k = \frac{Q(z_k)}{f'(z_k)}$$

Therefore, if the polynomial $Q(z)$ has rational coefficients and $z_k \in \mathbb{Q}$ are rational numbers, then the numbers a_k are also rational. ■

The following statement plays a very basic role in the proof of Theorem 1.

Proposition 3. Let

$$S_n = s^{n-1} \int_0^\infty (\sin^n x) e^{-sx} dx, n \in \mathbb{N}, s > 0$$

Then it holds

$$S_{n+2} = S_n \frac{(n+1)(n+2)}{((n+2)^2 + s^2)}$$

Therefore, if $n = 2m + 1$, $m \in \mathbb{N}$, is an odd number, then

$$S_n = \frac{n! (s^2)^m}{(s^2 + 1)(s^2 + 9) \cdots (s^2 + n^2)}$$

and if $n = 2m$, $m \in \mathbb{N}$, is an even number, then

$$S_n = \frac{n! (s^2)^{m-1}}{(s^2 + 4)(s^2 + 16) \cdots (s^2 + n^2)}$$

In the first case, the degree of the denominator as a function of s^2 is $m + 1$, and in the second case is m . In both cases, S_n is a proper rational function of s^2 .

Proof. The proof is based on successive transformations, using the technique of integration by parts.

$$\begin{aligned}
 S_{n+2} &= \int_0^{\infty} (\sin^{n+2} x) e^{-sx} dx \\
 &= \int_0^{\infty} (\sin^n x) (1 - \cos^2 x) e^{-sx} dx \\
 &= S_n - \int_0^{\infty} (\sin^n x) \cos^2 x e^{-sx} dx \\
 &= S_n - \int_0^{\infty} (\sin^n x) \cos x e^{-sx} d \sin x \\
 &= S_n - \frac{1}{n+1} \int_0^{\infty} \cos x e^{-sx} d \sin^{n+1} x \\
 &= S_n + \frac{1}{n+1} \int_0^{\infty} \sin^{n+1} x d \cos x e^{-sx} \\
 &= S_n + \frac{1}{n+1} \int_0^{\infty} (\sin^{n+1} x) (-\sin x e^{-sx} - s \cos x e^{-sx}) dx \\
 &= S_n + \frac{1}{n+1} \int_0^{\infty} (-\sin^{n+2} x e^{-sx} - s \sin^{n+1} x \cos x e^{-sx}) dx \\
 &= S_n - \frac{1}{n+1} \int_0^{\infty} \sin^{n+2} x e^{-sx} dx \\
 &\quad - \frac{s}{n+1} \int_0^{\infty} (\sin^{n+1} x \cos x e^{-sx}) dx \\
 &= S_n - \frac{S_{n+2}}{n+1} - \frac{s}{n+1} \int_0^{\infty} \sin^{n+1} x e^{-sx} d \sin x \\
 &= S_n - \frac{S_{n+2}}{n+1} - \frac{s}{(n+1)(n+2)} \int_0^{\infty} e^{-sx} d \sin^{n+2} x \\
 &= S_n - \frac{S_{n+2}}{n+1} + \frac{s}{(n+1)(n+2)} \int_0^{\infty} \sin^{n+2} x d e^{-sx} \\
 &= S_n - \frac{S_{n+2}}{n+1} \\
 &\quad + \frac{s}{(n+1)(n+2)} \int_0^{\infty} (\sin^{n+2} x) (-s e^{-sx}) dx \\
 &= S_n - \frac{S_{n+2}}{n+1} - \frac{s^2}{(n+1)(n+2)} \int_0^{\infty} (\sin^{n+2} x) (e^{-sx}) dx \\
 &= S_n - \frac{S_{n+2}}{n+1} - \frac{s^2}{(n+1)(n+2)} S_{n+2}
 \end{aligned}$$

Therefore

$$S_{n+2} = S_n - \frac{S_{n+2}}{n+1} - \frac{s^2}{(n+1)(n+2)} S_{n+2}$$

which implies the proof of Proposition 3. ■

Now we are at position to finish the proof of Theorem 1. Suppose that $n = 2m + 1$, $m \in \mathbb{N}$, is an odd number and put $s^2 = z$, $z_k = -(2k + 1)^2$, $0 \leq k \leq m$, $Q(z) = z^m$

$$f(z) = (z - z_0)(z - z_1) \cdots (z - z_m)$$

From Proposition 2 we obtain

$$\begin{aligned}
 S_n &= \frac{n! z^m}{f(z)} = n! \sum_{k=0}^m \left(\frac{Q(z_k)}{f'(z_k)} \right) \frac{1}{z - z_k} \\
 &= n! \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \frac{1}{s^2 + (2k + 1)^2}
 \end{aligned}$$

According to (1)

$$\begin{aligned}
 \mathcal{D}_n &= \frac{1}{\pi(n-1)!} \int_0^{\infty} S_n ds \\
 &= \frac{n!}{\pi(n-1)!} \int_0^{\infty} \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \frac{1}{s^2 + (2k + 1)^2} ds \\
 \mathcal{D}_n &= \frac{n}{\pi} \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \int_0^{\infty} \frac{1}{s^2 + (2k + 1)^2} ds \\
 \mathcal{D}_n &= \frac{n}{\pi} \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \left(\frac{\pi}{2(2k + 1)} \right) \\
 \mathcal{D}_n &= \frac{n}{2} \sum_{k=0}^m \left(\frac{z_k^m}{f'(z_k)} \right) \frac{1}{(2k + 1)} \Rightarrow \mathcal{D}_n \in \mathbb{Q} \quad (2)
 \end{aligned}$$

Now let $n = 2m$, $m \in \mathbb{N}$, be an even number and let $s^2 = z$, $z_k = -(2k)^2$, $1 \leq k \leq m$, $Q(z) = z^{m-1}$

$$f(z) = (z - z_1)(z - z_2) \cdots (z - z_m)$$

Then from Proposition 2 we obtain

$$\begin{aligned}
 S_n &= \frac{n! z^{m-1}}{f(z)} = n! \sum_{k=1}^m \left(\frac{Q(z_k)}{f'(z_k)} \right) \frac{1}{z - z_k} \\
 &= n! \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \frac{1}{s^2 + (2k)^2}
 \end{aligned}$$

Again, according to (1)

$$\begin{aligned}
 \mathcal{D}_n &= \frac{1}{\pi(n-1)!} \int_0^{\infty} S_n ds \\
 &= \frac{n!}{\pi(n-1)!} \int_0^{\infty} \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \frac{1}{s^2 + (2k)^2} ds \\
 \mathcal{D}_n &= \frac{n}{\pi} \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \int_0^{\infty} \frac{1}{s^2 + (2k)^2} ds \\
 &= \frac{n}{\pi} \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \left(\frac{\pi}{4k} \right)
 \end{aligned}$$

$$\mathcal{D}_n = \frac{n}{4} \sum_{k=1}^m \left(\frac{z_k^{m-1}}{f'(z_k)} \right) \frac{1}{k} \Rightarrow \mathcal{D}_n \in \mathbb{Q} \quad (3)$$

Relations (2) and (3) prove completely Theorem 1. ■

The authors of the present work perceive as an amazing fact the rational value of $\mathcal{D}_n \in \mathbb{Q}$ for any $n \in \mathbb{N}$. The uniqueness and significance of the fundamental integral $\mathcal{D}$ contains sufficient motivation to search various regularities related to it, revealing at the same time various discussion opportunities.

IV. LOBACHEVSKI INTEGRAL FORMULA

The integrals considered above are related to a remarkable formula, the content of which is given in the following theorem, presented for example in [9] and [10].

Theorem 2. Let the continuous (or locally integrable) function $f(x): \mathbb{R} \rightarrow \mathbb{R}$ satisfy the condition

$$f(\pi + x) = f(\pi - x) = f(x) \quad \forall x \in \mathbb{R}$$

Then

$$\int_0^\infty f(x) \frac{\sin^2 x}{x^2} dx = \int_0^\infty f(x) \frac{\sin x}{x} dx = \int_0^{\frac{\pi}{2}} f(x) dx \quad \blacksquare$$

By condition, the function $f(x)$ is even, because

$$f(-x) = f(\pi - (-x)) = f(\pi + x) = f(x)$$

and also π -periodic. A detailed proof of Theorem 2 can be found, for instance, in [9]. but the proof assumes a solid knowledge from an undergraduate course in mathematics. In particular, from Theorem 2 it follows that

$$\int_0^\infty \frac{\sin^2 x}{x^2} dx = \int_0^\infty \frac{\sin x}{x} dx = \frac{\pi}{2}$$

V. CONCLUSIONS

The improper conditionally convergent Dirichlet integral is always of great interest, as it is related to the convergence of the Fourier transform. This work describes approaches to some analytic calculations, for which we

modestly hope may appear to be useful also in other circumstances, potentially concerning digital signal processing.

VI. ACKNOWLEDGMENTS

The authors are grateful to the department colleagues for the support of this publication, which was developed in connection with the national project BG05M2OP001-2.016-0003 "Modernization of the National Military University "Vasil Levski" and Sofia University "St. Kliment Ohridski".

REFERENCES

- [1] R. G. Bartle, "Return to the Riemann Integral," The American Mathematical Monthly, vol. 103(8), pp. 625-632, 1996.
- [2] A. Zygmund, Trigonometric Series. 3rd edition, Foreword by Robert Fefferman, Cambridge University Press, 2003. <https://doi.org/10.1017/CBO9781316036587>
- [3] A. D. Poularikas, The Handbook of Formulas and Tables for Signal Processing, A CRC Handbook Published in Cooperation with IEEE Press, 1999.
- [4] L. C. Andrews and B. K. Shivamoggi, Integral Transforms for Engineers, New York: Macmillan, 1999. Available: <https://www.scribd.com/document/259005942/Integral-Transform-for-Engineers> [Accessed Dec. 08, 2025]
- [5] K. B. Wolf, Integral Transforms in Science and Engineering, New York: Springer, 1979.
- [6] W. Rudin, Real and Complex Analysis. Third Edition, McGraw-Hill Book Company, 1987. ISBN: 0-07-054234-1 [Online], Available: <https://perso.telecom-paristech.fr/decreuse/downloads/c22155fef582344beb326c1f44f437d2/rudin.pdf> [Accessed Dec. 08, 2025]
- [7] U-R. Kim, S. Cho and J. Lee, "The art of Schwinger and Feynman parametrizations," Journal of the Korean Physical Society, vol. 82, pp. 1023–1039, 2023. <https://doi.org/10.1007/s40042-023-00764-3>
- [8] Z. Burghilea, "Feynman's Trick," December. 08, 2025. [Online]. Available: <https://zackyyz.github.io/feynman.html> [Accessed: Dec. 08, 2025].
- [9] "Lobachevsky's Formula for Integrals," December. 08, 2025. [Online]. Available: <https://math.stackexchange.com/questions/776903/lobachevskys-formula-for-integrals> [Accessed: Dec. 08, 2025].
- [10] H. Jolany, "An extension of the Lobachevsky formula", Elem. Math., Vol. 73 (3), pp. 89–94, 2018. <https://doi.org/10.4171/EM/358>

An Optimized Model for CPU Load Evaluation in the Execution of Code Structures and Script-Based Algorithms

Valentin Atanasov

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
v.atanasov@shu.bg

Daniel Denev

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
d.denev@shu.bg

Abstract. The introduction of models for studying the impact of script-based algorithms in web applications on overall CPU load should occupy an important place in the modern communication environment. However, there is a limited availability of software tools in this field. By exploring this subject, a team of researchers in the area of web applications developed a model with key characteristics representing scalar values of indicators that describe CPU load. This developed model for evaluating scalar time-based metrics has undergone evolution and optimization, expressed in increased accuracy of metrics, improved process stability, enhanced precision of results, and, not least, greater efficiency in user perception. This paper presents an optimized model for evaluating CPU load during the execution of code structures and script algorithms.

Keywords: Benchmark CPU Algorithm, CPU load, WEB applications, JavaScript, Code Algorithms, DOM.

I. INTRODUCTION

The operation of modern web browsers is based on clearly defined stages of content processing and rendering, which together form the computational pipeline. Instead of simplified models that describe the browser as a collection of separate “machines,” contemporary literature adopts a process-oriented approach.

In this context, the following main stages can be distinguished: resource fetching (networking), parsing of HTML and CSS documents, construction of the DOM and CSSOM tree structures, execution of JavaScript code by the JavaScript engine, style calculation, layout (reflow), and the final stage—rendering through painting and compositing.

CPU load during the execution of client-side scripts is directly related to the algorithmic complexity of these stages, particularly with respect to DOM operations, layout recalculation frequency, and the complexity of the

executed JavaScript algorithms. In this context, the execution time of individual operations represents a key indicator of web application performance in a client-side environment.

There is a growing trend in the use of the scripting language JavaScript, with a steady increase [1], [2], [4]–[6] in web-based applications. This trend is driven, on the one hand, by the dynamic development of web technologies and the HTML5 suite, and on the other hand, by the total dominance of a key user characteristic—a high degree of interactivity demanded by a highly interactive generation.

With the rapid development of web technologies, JavaScript-based applications, and browser engines, there has been a continuous evolution of models and approaches for analyzing and optimizing computational performance in client-side environments. Each successive generation of benchmarking methodologies builds upon previous approaches by introducing improved mechanisms for measuring execution time, rendering performance, and resource utilization in increasingly complex web systems. One of the most effective directions in this field is the use of structured stress-testing models and deterministic measurement pipelines, which allow more accurate evaluation of CPU load and browser rendering behavior under controlled conditions. In earlier stages of research and practice, performance evaluation of web applications was primarily based on simple timing functions and isolated execution measurements. However, these approaches often lacked sufficient precision, reproducibility, and the ability to capture the full complexity of modern browser pipelines, including the interactions between JavaScript execution, DOM manipulation, CSSOM processing, and rendering stages such as layout, reflow, and repaint. With the increasing complexity of web applications and the growing demand

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.137>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

for highly interactive user experiences, the need for more advanced and systematic benchmarking techniques has become evident.

In our scientific research, we review several key contributions in this field. Canay and Kocabiçak [1] explore augmented web usage mining and user experience optimization, emphasizing the importance of enriched analytics data for understanding user interaction patterns in web environments. Xavier [2] presents a quantitative analysis of global web usage, providing insight into large-scale behavioral trends that influence modern web application design and optimization strategies. Atanasov [3] focuses on approaches for evaluating code algorithms in web applications, introducing foundational concepts related to performance measurement and computational analysis in browser-based systems.

Additionally, industry-driven statistical reports [4], [5], [6] highlight the dominant role of JavaScript and related web technologies in contemporary software development, confirming the necessity of efficient performance evaluation tools. Standardization documents such as the DOM Living Standard [7] and CSS Object Model specifications [8] provide the structural basis for understanding how browsers construct and manipulate document representations. Furthermore, Mozilla's documentation on browser internals [9] offers essential insight into the rendering pipeline and the stages influencing runtime performance.

Collectively, these studies demonstrate that modern performance evaluation in web environments requires a combination of empirical measurement, architectural understanding, and statistical analysis. The proposed model extends these foundations by introducing a sandboxed, repeatable, and statistically stabilized benchmarking approach tailored for DOM and JavaScript stress-testing scenarios [11], [14].

II. MATERIALS AND METHODS

Experimental Setup – Code Component

A university research team analyzed a developed model of a web-based prototype application that examines CPU load during the execution of JavaScript code algorithms for the following set of indicators [3]:

- measurement of performance metrics;
- JavaScript execution time;
- render time;
- layout time;
- reflow / repaint measurements;
- analysis of inefficient DOM manipulations;
- asynchronous operation timing;
- graphical visualization of timing data;
- system logging;
- isolated (sandboxed) execution within an iframe.

The architecture of the developed application was based on two interconnected models—the Document Object Model (DOM) [7] and the Cascading Style Sheets

Object Model (CSSOM) [8]. The main set of approaches included:

- execution of user-provided HTML and JavaScript code within a sandboxed iframe;
- isolation of user code;
- measurement of HTML document load time and JavaScript execution time;
- use of `performance.now()`;
- use of `setTimeout` and `setInterval`;
- blocking of `Promise` and `fetch`;
- real-time updates;
- suitability for micro-benchmarks;
- interception of `console.log`;
- capability to stop dynamic content updates, clear, and reload the virtual environment.

As functionally complete injected code components, a web-based application featuring a complex DOM structure and a JavaScript algorithm simulating an educational TCP three-way handshake scenario was used.

III. RESULTS AND DISCUSSION

Without going into the details of the subsystem modules in the architecture, a summarized set of analytical results from the empirical study of the web-based benchmark prototype is presented:

- The evaluation module of the studied prototype produced observed data in accordance with the designed functionality, along with partial conclusions regarding the use of `setInterval` instead of `requestAnimationFrame`, and the resulting logical relationship between Reflow and Repaint;
- During the code evaluation, for $x \in X$ a failure $F(x)$ of the client agent was observed, caused by the following logical chain:

$$\forall x(\exists x(H(x) \wedge E(x, 250) \wedge L(x) \wedge D(x) \wedge C(x)) \rightarrow F(x))$$

where:

$H(x)$ = x heavy engine

$E(x, n)$ = x has n executions

$L(x)$

= x uses `setInterval` and has memory leaks

$D(x)$

= x the algorithm performs frequent DOM rebuilds

$C(x)$

= x the algorithm performs canvas rendering

$F(x)$ = x leads to crash / high CPU usage / hang

By analyzing the empirical phase, the following conclusions were drawn for the web-based benchmark prototype:

1. Monolithic Execution

- The examined model directly executes JavaScript (new `Function(js)`), which blocks the UI and makes the benchmark unstable.
- All executions of user code should be sandboxed, for example in a Web

Worker, in order to isolate and protect the Main Thread and the interface.

2. Mixing of Responsibilities

- The benchmark combines: UI, code execution, statistics, and quality analysis.
- Code logic, interface, analysis, and statistics should be modular, with clearly separated responsibilities.

1. Unoptimized Loops and Visualization

- In the code, each iteration updates the DOM/graphics, which is CPU-intensive.
- Batching and throttling in visualization reduce unnecessary load.

2. Lack of Resource Lifecycle Management

- Multiple intervals and DOM elements are created without cleanup, leading to memory leaks.
- Each resource creation should have a clearly defined lifecycle: initialization → usage → cleanup.

3. Inefficient Statistics and Reporting

- Statistics such as p95, p99, and standard deviation are not collected, which complicates result interpretation.
- Collecting comprehensive statistical indicators improves performance evaluation.

4. Risk of Problematic Code

- Without static analysis, checks for infinite loops, setInterval without clear, event listener leaks, and DOM manipulation in loops, the benchmark may crash.
- A static analyzer and heuristics for code smells protect the tool from failure under heavy code.

5. Approximate CPU Load Estimation

- JavaScript does not provide a direct API for CPU usage.
- Measurement should be based on execution time/wall time, with proper adjustment for frame budget.

Based on the obtained conclusions, an optimization phase was initiated, whose architecture is presented in Fig.1.

The architecture shown in Fig.1 covers the following main tasks:

- construction of a deterministic sandbox environment for execution, which guarantees identical initial conditions and isolation of user code;
- creation of a signal amplification mechanism that makes micro-measurements of JavaScript execution reliable and measurable;

- implementation of a two-layer measurement approach that separates JavaScript execution from render/pipeline latency in the browser;
- development of a statistical pipeline for noise reduction, including aggregation and stabilization of results through metrics such as median, percentile values, and variance, in order to obtain repeatable and interpretable performance results.

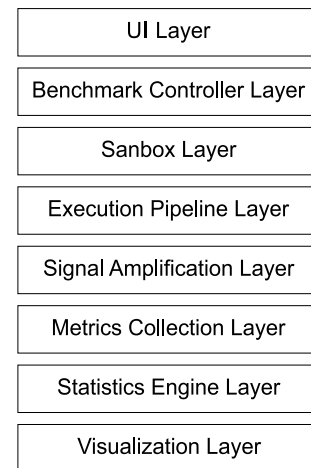


Fig. 1. Architecture of the Optimized Model for a Repeatable DOM & JS Stress Harness with Statistical Output.

As a result of these tasks, the model for a repeatable DOM & JS stress harness with statistical output was further optimized. This optimization phase was followed by code development, which was subjected to a series of tests. One of the main advantages of the optimized code is the high-precision measurement of individual JavaScript operations through the use of `performance.now()`, which provides millisecond-level accuracy. To support the above with statistical arguments, we will compare two methods, the first, `removeOutliers(5%)`, is applied in the non-optimized model, while the second (10%) is applied in the optimized model. The `removeOutliers(5%)` method, after sorting, removes one value from each extreme (the lowest and the highest), which may be useful for small datasets but is not always sufficiently valid for larger datasets with many deviations. The second method, `trim(10%)`, removes 10% of the values from each extreme after sorting and provides improved data stability, making it more suitable for realistic and robust measurements in browser testing and performance analysis. Both methods aim to eliminate extreme anomalies that may introduce noise and distort statistical indicators such as the median, standard deviation, and percentile values. The proposed algorithm of the mathematical apparatus used to remove data points that significantly deviate from the main distribution and are not considered representative of the normal behavior of the data is presented in Table 1 [12].

TABLE 1 SCRIPT-BASED ALGORITHM OF THE MATHEMATICAL APPARATUS FOR TRIMMING THE LOWEST AND HIGHEST DATA VALUES

```
// Data trimming method – removes the lowest and
// highest 10% of values
function trim(arr, ratio = 0.1) {
// Check if the dataset has fewer than 10 values; in that
// case, trimming is not applied
if (arr.length < 10) return arr;
// Sort the data
const sorted = [...arr].sort((a, b) => a - b);
// Calculate the number of values to remove (10%)
const cut = Math.floor(arr.length * ratio);
// Return the data without the lowest and highest 10%
return sorted.slice(cut, sorted.length - cut);
}
```

To ensure the validity of the statistical analysis, an identical population of 300 input values is assumed for both methods. Using statistical processing techniques, the following procedure is applied:

- Generation of 300 random data points from a normal distribution.
- Application of the two data filtering methods: removeOutliers(5%) and trim(10%).
- Calculation of statistical indicators: median, standard deviation, p95, standard error, and confidence interval.
- Conducting a Levene's test to assess differences in variability between the two methods.
- Comparing precision through the standard error (SE) and the width of the confidence interval.

The conducted test generates output data summarized in Table 2. Figure 2, Figure 3, Figure 4, Figure 5 compare the key statistical metrics between the two data processing approaches: removeOutliers (5%) and trim (10%). They visually demonstrate how trimming improves stability, reduces variability, and provides more reliable estimates across all evaluated indicators.

TABLE 2 GENERATED OUTPUT DATA FROM THE STATISTICAL ANALYSIS OF THE METHODS REMOVEOUTLIERS (5%) AND TRIM (10%)

Metric	removeOutliers (5%)	trim (10%)	Difference / Improvement
Median	0.05922	0.05922	0.00% (stable)
Standard deviation	0.75953	0.63363	-16.58% noise
p95 (Upper bound)	1.16111	0.95447	-17.80%
Standard error (SE)	0.04622	0.04090	-11.52% error
95% confidence interval	[-0.109, 0.073]	[-0.103, 0.058]	More focused range
Confidence interval width	0.18201	0.16114	-11.47% narrower

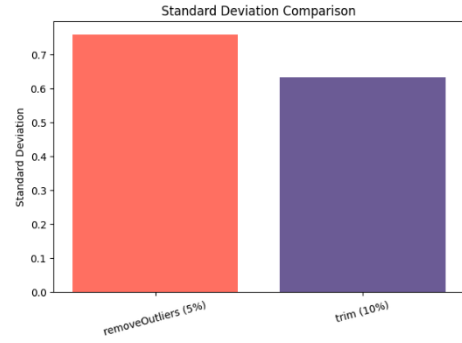


Fig. 2. Standard Deviation Comparison.

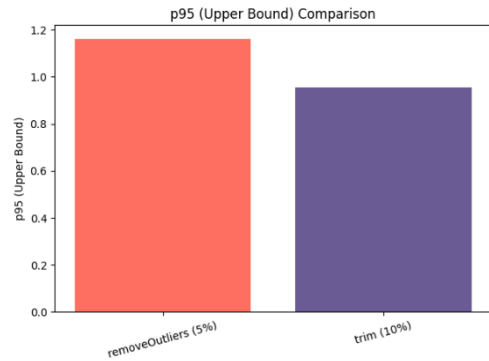


Fig. 3. Standard Deviation Comparison.



Fig. 4. Standard Error (SE) Comparison.



Fig. 5. Confidence Interval Width Comparison.

With the data thus formed and summarized in Table 2, the probable conclusions from the analysis of these data are presented in Table 3.

TABLE 3 ANALYSIS OF THE STATISTICAL RESULTS FROM THE COMPARISON OF THE METHODS REMOVEOUTLIERS (5%) AND TRIM (10%)

Evidence	Value / Result	Conclusions
Levene Test (p-value)	0.00545	The difference is statistically significant ($p < 0.05$). The factor of randomness is excluded.
Stable deviation	16.58% lower	Data under trim(10%) is significantly more homogeneous and cleaned from anomalies.
Precision (SE)	11.52% improvement	The estimate of the mean value is more reliable and robust to new data.
Reliability (CI)	11.47% narrower interval	Higher confidence in predicting results.

Based on the analysis of the processed data, the efficiency index ε is defined as a relative measure. It serves as an indicator of accuracy in terms of reduced noise when transitioning from one filtering method to another. This index is expressed by the following mathematical formulation:

$$\varepsilon = \frac{\sigma_{5\%} - \sigma_{10\%}}{\sigma_{5\%}}$$

where:

$\sigma_{5\%}$ is the standard deviation with 5% outlier removal (0.75953)

$\sigma_{10\%}$ is the standard deviation with 10% trimming (0.63363)

The final conclusion can be summarized as follows:

This index $\varepsilon \approx 16.58\%$ can be interpreted as evidence of the higher precision and stability of the trim(10%) method within the optimized model. There is also a reduction in uncertainty when using the trim(10%) method, which reduces data variability by over 16%. A higher efficiency index ε implies that in subsequent iterations of the experiment with new sets of 300 data points, the results obtained using trim(10%) are less likely to deviate from the original baseline compared to those obtained using the removeOutliers(5%) method. The trim(10%) method achieves a 16.58% improvement in the reliability of the optimized model, demonstrated through statistical variance optimization.

IV. CONCLUSION

Based on the analysis of the prototype, the authors conclude that the examined system provides a deterministic measurement pipeline and a browser sandbox execution environment, in which the main execution flows are separated into execution (Sandbox & Pipeline), measurement (Amplification & Metrics), interpretation (Statistics), and presentation (Visualization). The evolution of the mathematical apparatus for trimming extreme values (outliers), traditionally implemented through statistical software such as R, Python (with libraries like NumPy or Pandas), and MATLAB, has led to its implementation in

JavaScript as well. This enables web application developers to perform statistical analyses directly within the browser environment without requiring server-side solutions.

In addition to the conclusions drawn, it can be noted that the proposed model demonstrates the possibility of portability and adaptation to different types of web applications and load scenarios, including both synthetic benchmark tests and real user interactions. This makes the proposed model suitable not only as a research tool, but also as a foundation for future systems for performance monitoring and analysis in client-side environments.

Of additional significance is the fact that separating the core processes into distinct logical layers enables a clearer interpretation of results and easier identification of sources of performance degradation. In this way, the model creates prerequisites for improved diagnosis of complex interactions between JavaScript execution and the browser rendering pipeline.

From the perspective of future development, the model can be extended through the introduction of automated mechanisms for adaptive load generation, where test scenarios change dynamically depending on the observed behavior of the system. This would enable more realistic load simulation and higher sensitivity to edge cases.

Furthermore, the integration of more advanced analytical methods and intelligent algorithms for pattern recognition in the collected metrics could contribute to a deeper understanding of the dependencies between different execution layers. In this context, the model has the potential to evolve into an autonomous system for evaluating and predicting performance in web-based environments [10], [13].

V. ACKNOWLEDGEMENT

In this section of the present study, the authors would like to express their sincere gratitude to all colleagues from the department for their continuous support, constructive discussions, and valuable technical feedback throughout the development and optimization of the proposed web-based benchmarking model. Their expertise and recommendations were essential for refining the methodological approach and improving the overall reliability of the experimental framework. We also extend our deep appreciation to our families for their constant encouragement, understanding, and patience, which provided strong motivation during the research and development process. This publication is funded by the fund "Support for Publishing Publications in Journals with Impact Factor (IF) and Impact Rank (SJR)" of Konstantin Preslavsky University of Shumen, Republic of Bulgaria.

REFERENCES

- [1] Ö. Canay and Ü. Kocabaşak, "Augmented web usage mining and user experience optimization with CAWAL's enriched analytics data," *International Journal of Human-Computer Interaction*, vol. 41, no. 11, pp. 7152–7171, 2025, doi: <https://doi.org/10.1080/10447318.2025.2495839>.

- [2] H. S. Xavier, "The web unpacked: a quantitative analysis of global web usage," in *Proc. 20th Int. Conf. Web Information Systems and Technologies (WEBIST)*, 2024, pp. 183–190, doi: <https://doi.org/10.5220/0012905900003825>.
- [3] V. T. Atanasov, "An approach to evaluating code algorithms in web applications," *Annual of Konstantin Preslavsky University of Shumen*, vol. XV E, pp. 25–31, 2025, doi: <https://doi.org/10.46687/YT25VTA>.
- [4] "Comparison of the usage statistics of JavaScript for websites," W3Techs, 2026. [Online]. Available: <https://w3techs.com/technologies/comparison/cp-javascript>. [Accessed: Apr. 6, 2026].
- [5] "Most used programming languages among developers worldwide as of 2025," Statista, 2025. [Online]. Available: <https://www.statista.com/statistics/793628/worldwide-developer-survey-most-used-languages/>. [Accessed: Apr. 6, 2026].
- [6] "Most popular technologies," Stack Exchange Inc., 2025. [Online]. Available: <https://survey.stackoverflow.co/2024/technology>. [Accessed: Apr. 6, 2026].
- [7] Web Hypertext Application Technology Working Group, "DOM Living Standard," 2026. [Online]. Available: <https://dom.spec.whatwg.org/>. [Accessed: Apr. 6, 2026].
- [8] Mozilla Corporation, "CSS Object Model (CSSOM)," 2026. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/CSS_Object_Model. [Accessed: Apr. 6, 2026].
- [9] Mozilla Corporation, "How browsers work," 2026. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/Performance/Guides/How_browsers_work. [Accessed: Apr. 6, 2026].
- [10] Ts. Tsankov, L. Staneva, I. Vardeva, and D. Iliev, "Generalized net model of a communication network using the Port Knocking method," in *Proc. Scientific Conf. MATTEH 2022*, vol. 2, Shumen, Bulgaria, 2022, pp. 29–34.
- [11] Ts. Tsankov, L. Staneva, I. Vardeva, and D. Iliev, "Application of a generalized net model in the communication of two independent traffic," in *Proc. 15th Int. Scientific Conf. Environment. Technology. Resources*, vol. II, Rezekne, Latvia, 2024, pp. 293–296.
- [12] V. Stoyanova, "Research of the characteristics of a steganography algorithm in images when using different alphabet," in *Proc. 15th Int. Scientific and Practical Conf.*, vol. IV, 2024, p. 259.
- [13] V. T. Stoyanova, "Steganography system using more LSBs," *ENTRENOVA – Enterprise Research Innovation*, vol. 4, no. 1, pp. 168–174, 2018.
- [14] K. Kalchev and Ts. Tsankov, "Use of the decision tree method in analysis of student data from surveys," *Annual of Konstantin Preslavsky University of Shumen*, vol. X E, pp. 72–75, 2020.

WEB Traffic Management by Techniques with Support Vector Machine, Naïve Bayes and Discriminant Analysis

Ivelina Balabanova

Dept. of Communications Equipment
and Technologies
Technical University of Gabrovo
Gabrovo, Bulgaria
ivstoeva@abv.bg

Desislava Petrova

Dept. of Management
Technical University of Gabrovo
Gabrovo, Bulgaria
des_petrova@abv.bg

Georgi Georgiev

Dept. of Communications Equipment
and Technologies
Technical University of Gabrovo
Gabrovo, Bulgaria
givanow@abv.bg

Abstract—Effective diagnostics of WEB services distribution is an important prerequisite for adequate traffic load service planning in information and communication infrastructures in serving corporate clients. Network administrators play a key role in specification and transmission medium metrics analysis in web traffic management. The paper proposes a Machine Learning approach for WEB traffic streams diagnostics and categorization of corporate business clients in urban areas. The approach envisages a pre-processing phase in network traffic analysis procedures, incorporating the following specific traffic metrics: Flows, IPv4 Packet size, IPv4 Packet size distribution, and Mean Transition Rate. The second stage of the research integrates analytical tools based on Support Vector Machine (SVM), Naïve Bayes (NB) algorithm, Linear Discriminant Analysis (LDA), and Quadratic Discriminant Analysis (QDA). The effectiveness of a system comprising C-SVM and Nu-SVM classifiers was evaluated using different sets of Kernel functions - Linear, Polynomial, Radial Basis Function (RBF), and Sigmoid types were applied. An advantage for Nu-SVM WEB traffic classification processes was established, where a maximum threshold recognition of 100.00% was achieved for the target classification groups defined. NB classifier training processes were conducted by Normal, Lognormal, Gamma and Poisson distributions applied to the input datasets. The highest classification accuracy of 100.00% was obtained for the Normal distribution, whereas when training the NB classifier with the Lognormal data distribution a significant reduction in this criterion below the 36.00% threshold was observed. Training and verification series of procedures were performed for Discriminant classifiers, respectively LDA, Diagonal Linear Discriminant Analysis (DLDA), Pseudo-Linear Discriminant Analysis (PLDA), QDA, Diagonal Quadratic Discriminant Analysis (DQDA) and Pseudo-Quadratic Discriminant Analysis (PQDA). In performance evaluation for the defined Linear and Quadratic types of DA classifiers, the highest recognition threshold of 90.00% was

achieved in the WEB traffic streams analyzed in the case of PLDA classification procedures.

Keywords—network monitoring; WEB traffic, urban area, C-SVM, Nu-SVM, Naïve Bayes; linear DA, quadratic DA.

I. INTRODUCTION

Ensuring adequate quality of service for private and corporate clients in WEB Traffic and Network Resources parametrization encompasses a number of specific activities. Some of the most important ones that can be mentioned are:

- Network traffic classification and prediction;
- Effective traffic routing and network security;
- Network performance and data integrity support;
- Error control in transmission media surcharge, [1-4] etc.

The implementation of analytical approaches for network diagnostics will further expand the spectrum of developers' capabilities for modeling and evaluating:

- Communication channel specification, noise control in transmitter and receiver services;
- Effective traffic load monitoring in structural network resources;
- Local coverage geographical areas assessment;
- Reliability and services prioritization in broadband Internet access planning [5-7].

More specifically, tools based on Artificial Intelligence, Machine Learning and Deep Learning concepts have been used to evaluate various processes regarding the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.122>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

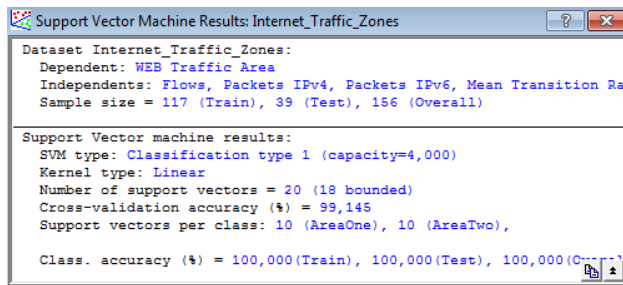
effectiveness of the communication infrastructure, as follows:

- Channel estimation: DNN (Deep Neural Networks), LSTM (Long-Short Term Memory) – a variant of RNN (Recurrent Neural Network);
- Channel prediction: Deep Neural Networks and CNN (Convolutional Neural Networks);
- Channel coding: Deep Neural Networks;
- Link adaptation: SVM (Support Vector Machine), k-NN (k – Nearest Neighbors);
- Reflecting intelligent surfaces (RIS): Deep Neural Networks;
- Spectrum sensing: k-Means, GMM (Gaussian Mixture Models), Support Vector Machine, k-Nearest Neighbors, Convolutional Neural Networks [8-12].

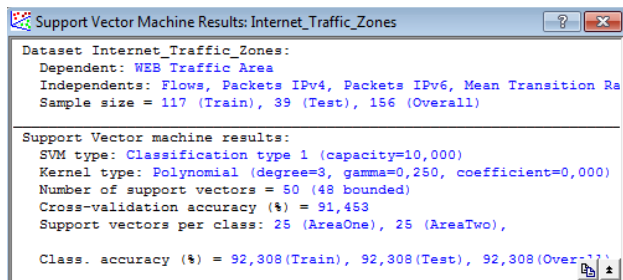
The paper proposes an approach based on Machine Learning methods and algorithms Support Vector Machine, Naïve Bayes and Discriminant Analysis for diagnosing the distribution of WEB services within active time zone in urban area for private and corporate clients.

II. SYNTHESIS OF SVM MODELS FOR WEB TRAFFIC AREA IDENTIFICATION IN STATISTICA

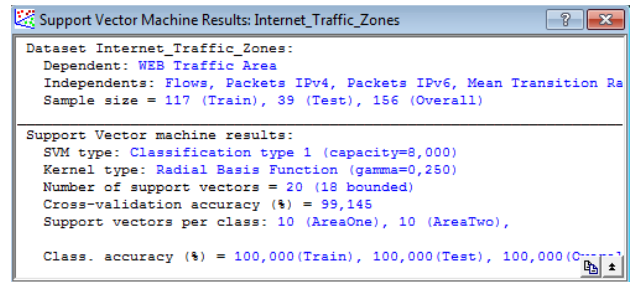
The first phase of the research is aimed at assessing the applicability of the SVM method on the defined task of diagnosing regions of consumption of accessible WEB content in urban environments. Two categories of SVM classifiers are adapted, respectively C-SVM and Nu-SVM. The evaluation of the functionality of the first group of classifiers was carried out under the following conditions: "Linear"; "Polynomial"; "RBF" and "Sigmoid" Kernel functions, shown in Fig. 1.



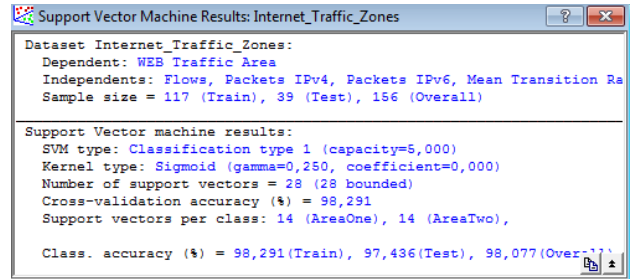
a)



b)



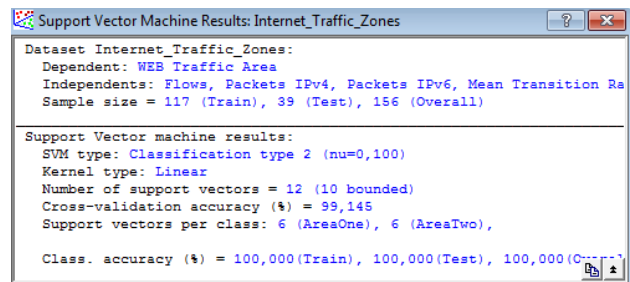
c)



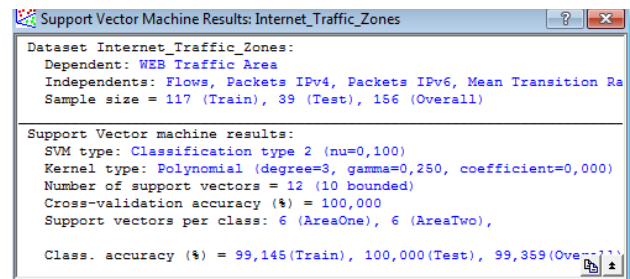
d)

Fig. 1. C-SVM classifiers for WEB traffic area recognition.

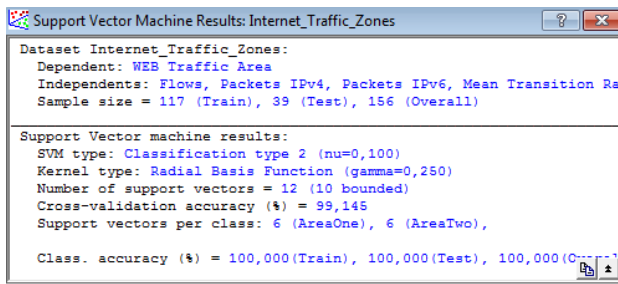
The necessary "Support Vectors" for constructing the "Hypersurface" separating the target output groups in the classification space, respectively "20", "50", "20" and "28", were analytically determined. The lowest final accuracy of 92.308 % was established for the C-SVM model with the applied Kernel function "Polynomial". A complete correct recognition of 100.0 % of the standards participating in the training and test datasets has been achieved, matching for the cases of "Linear" and "RBF", while in "Sigmoid" Kernel type final reported accuracy is 98.077 %.



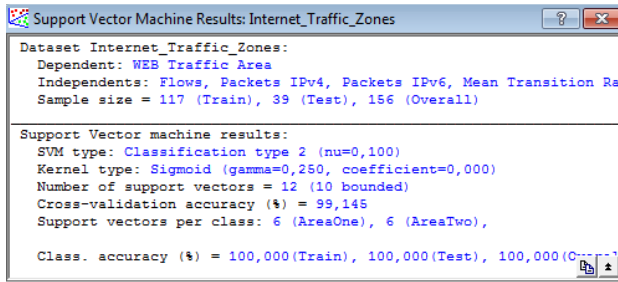
a)



b)



c)



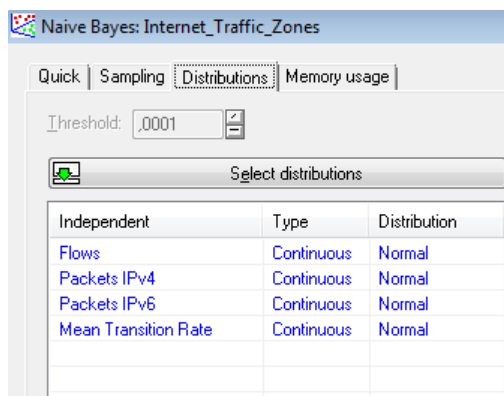
d)

Fig. 2. Nu-SVM classification models in WEB traffic area monitoring.

The possibility of adapting Nu-SVM classification models with respect to analogous types of Kernel functions was evaluated with some advantage, shown in Fig. 2. The maximum recognition threshold of 100.0% was reached for “Linear”, “Radial Basis Function” and “Sigmoid” Kernel functions. The final accuracy obtained with the Nu-SVM model using the “Polynomial” type set is 99.359 %.

III. NAÏVE BAYES CLASSIFICATION MODEL ANALYSIS IN WEB TRAFFIC MONITORING PROCEDURES IN STATISTICA

The second phase of the research consists of evaluating the suitability of the Naïve Bayes algorithm for four different types of distributions of variables in input datasets, related to the task of recognizing Internet usage zones and traffic load of network resources for corporate clients. The following types of data distributions were applied, respectively: “Normal”; “Lognormal”; “Gamma” and “Poisson”, given in Fig. 3.a), Fig. 4.a), Fig. 5.a), and Fig. 6.a).



a)

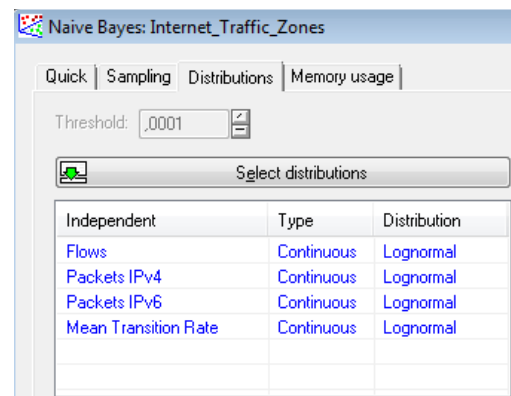
Naive Bayes model, WEB Traffic Area (Internet_Traffic_Zones)					
Class Name	Prior values	Flows Mean	Flows Standard deviation	Packets IPv4 Mean	Packets IPv4 Standard deviation
AreaOne	0.307692	125.9167	200.3643	123.2222	180.6921
AreaTwo	0.692308	200.5679	973.7235	179.9012	819.8901

b)

Classification summary (Naive Bayes Classifier), WEB					
Class Name	Total	Correct	Incorrect	Correct(%)	Incorrect(%)
AreaOne	14	14	0	100.0000	0.00
AreaTwo	25	25	0	100.0000	0.00

c)

Fig. 3. NB classifier in Normal distribution – a) distribution type, b) statistical metrics and c) confusion matrix.



a)

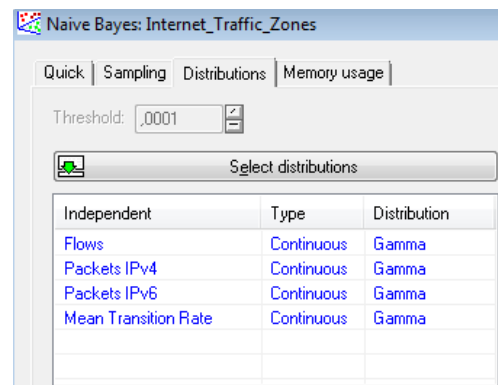
Naive Bayes model, WEB Traffic Area (Internet_Traffic_Zones)					
Class Name	Prior values	Flows Scale	Flows Shape	Packets IPv4 Scale	Packets IPv4 Shape
AreaOne	0.307692	66.99912	1.123335	69.42450	1.071214
AreaTwo	0.692308	40.46357	1.789274	38.55687	1.755149

b)

Classification summary (Naive Bayes Classifier), WEB					
Class Name	Total	Correct	Incorrect	Correct(%)	Incorrect(%)
AreaOne	39	14	25	35.89744	64.10256
AreaTwo	0	0	0	0.00000	0.00000

c)

Fig. 4. NB classification model in Lognormal distribution of input variables – a) distribution type, b) statistical metrics and c) confusion matrix.



a)

Naive Bayes model, WEB Traffic Area (Internet Traffic Zones)					
Class Name	Prior values	Flows Scale	Flows Shape	Packets IPv4 Scale	Packets IPv4 Shape
AreaOne	0.307692	318.829	0.394935	264.965	0.465050
AreaTwo	0.692308	4727.264	0.042428	3736.605	0.048146

b)

Classification summary (Naive Bayes Classifier), WEB					
Class Name	Total	Correct	Incorrect	Correct(%)	Incorrect(%)
AreaOne	0	0	0	0.00000	0.00000
AreaTwo	39	25	14	64.10256	35.89744

c)

Fig. 5. NB classifier at Gamma data distribution – a) distribution type, b) statistical metrics and c) confusion matrix.

Statistical metrics “Mean” and “Standard Deviation” were calculated for each input feature, as follows “Flows”, “IPv4 Packet size”, “Packets in IPv6” and “Mean Transition Rate”. The analytical indicators extracted from the quantitative analysis are given in Fig 3.b), Fig. 4.b), Fig. 5.b), and Fig. 6.b).

Naive Bayes: Internet_Traffic_Zones		
Quick	Sampling	Distributions
Threshold: .0001		
Select distributions		
Independent	Type	Distribution
Flows	Continuous	Poisson
Packets IPv4	Continuous	Poisson
Packets IPv6	Continuous	Poisson
Mean Transition Rate	Continuous	Poisson

a)

Naive Bayes model, WEB Traffic Area (Internet Traffic)				
Class Name	Prior values	Flows Shape	Packets IPv4 Shape	Packets IPv6 Shape
AreaOne	0.307692	125.9167	123.2222	123.6667
AreaTwo	0.692308	200.5679	179.9012	182.0741

b)

Classification summary (Naive Bayes Classifier), WEB					
Class Name	Total	Correct	Incorrect	Correct(%)	Incorrect(%)
AreaOne	17	14	3	82.3529	17.64706
AreaTwo	22	22	0	100.0000	0.00000

c)

Fig. 6. NB classification model at Poisson distribution of input variables -a) distribution type, b) statistical metrics and c) confusion matrix.

According to the “Normal” distribution of informative features, correct classification of the informative standards from both source groups was reported. With “Lognormal” data distribution, 25 samples from “Class № 2” were incorrectly assigned to samples from “Class № 1”. In the case of “Gamma” distribution, 14 samples included in

“Class № 1” were characterized by incorrectly determined membership to the composition of “Class № 2”. Regarding the last applied input dataset distribution, 3 samples from the structure of “Class № 2” were incorrectly assigned to the composition of the first output group. The obtained evaluation results show the highest degree of applicability to a standard “Normal” data distribution, confirmed in Fig. 3.c), Fig. 4.c), Fig. 5.c), and Fig. 6.c).

IV. EFFICIENCY ANALYS OF LINEAR AND QUADRATIC DISCRIMINANT CLASSIFIERS FOR WEB TRAFFIC DIAGNOSTICS IN MATLAB

The third phase of the research is based on evaluating the effectiveness of the created “Linear” and “Quadratic” Discriminant classification models in WEB Traffic monitoring procedures. The “Linear”, “Diagonal Linear”, “Pseudo-Linear”, “Quadratic”, “Diagonal Quadratic” and „Pseudo-Quadratic“ were successively evaluated. Table 1 summarizes the results for the studied discriminant models, confirming good and comparable achieved efficiency above 85.0 % levels.

TABLE I. ASSESSMENT METRICS IN EXAMINING THE QUALITY OF DISCRIMINANT CLASSIFIERS IN WEB TRAFFIC MONITORING

№	Evaluation Techniques		
	Type of Discriminant Classifier	Cross-Validation Loss	Cross-Validation Accuracy, %
1.	Linear	0.1026	89.47
2.	Diagonal Linear	0.1218	87.82
3.	Pseudo-Linear	0.0962	90.38
4.	Quadratic	0.1154	88.46
5.	Diagonal Quadratic	0.1218	87.82
6.	Pseudo-Quadratic	0.1026	89.74

Variables - DAModel			
DAModel			
Tx1 ClassificationDiscriminant			
Property	Value	Min	Max
XCentered	156x4 double	-683.1964	899.2308
Y	156x1 cell		
X	156x4 double	2.4000	1260
W	156x1 double	0.0064	0.0064
ModelParameters	1x1 classreg.learn...		
NumObservations	156	156	156
PredictorNames	1x4 cell		
CategoricalPredictors	[]		
ResponseName	'Y'		
ClassNames	2x1 cell		
Prior	[0.5000 0.5000]	0.5000	0.5000
Cost	[0 1; 1 0]	0	1
ScoreTransform	'none'		
DiscrimType	'pseudoLinear'		
Gamma	0	0	0
Delta	0	0	0
Coeffs	2x2 struct		
Mu	[9.2324 691.0364 ...	9.2324	861.9615
Sigma	4x4 double	-3.4249e...	8.2681e+04

a)

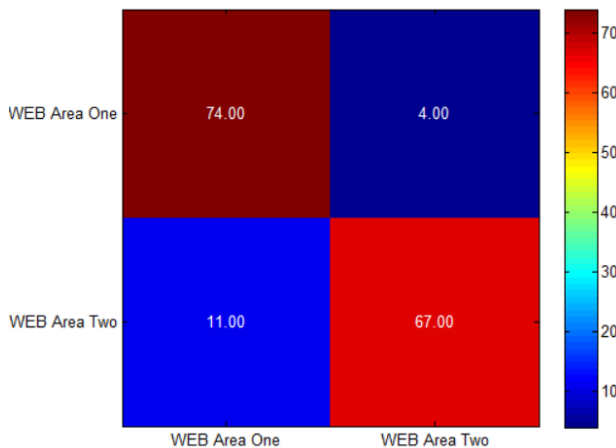
Variables - DAModel			
DAModel			
1x1 ClassificationDiscriminant			
Property	Value	Min	Max
XCentered	156x4 double	-683.1964	899.2308
Y	156x1 cell		
X	156x4 double	2.4000	1260
W	156x1 double	0.0064	0.0064
ModelParameters	1x1 classreg.learn...		
NumObservations	156	156	156
PredictorNames	1x4 cell		
CategoricalPredictors	[]		
ResponseName	'Y'		
ClassNames	2x1 cell		
Prior	[0.5000 0.5000]	0.5000	0.5000
Cost	[0 1; 1 0]	0	1
ScoreTransform	'none'		
DiscrimType	'diagQuadratic'		
Gamma	1	1	1
Delta	0	0	0
Coeffs	2x2 struct		
Mu	[9.2324 691.0364 ...]	9.2324	861.9615
Sigma	1x4x2 double	20.2860	9.6436e+04

b)

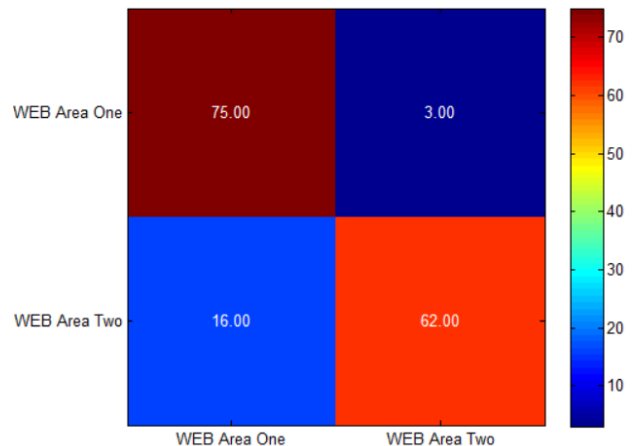
Fig. 7. Statistical indicators computed in a) “Pseudo-Linear” and b) “Diagonal Quadratic” model assessment.

The lowest classification accuracy of 87.82 % was reported for the cases of „Diagonal Linear“ and „Diagonal Quadratic“ discriminant type. The best adequacy to the specificity of the classification task was observed for „Pseudo-Linear“ model, expressed with a quantitative assessment of 90.38 %.

The set of specific statistical metrics computed in the course of studying the constructed Discriminant Classifiers shows the highest efficiency obtained in the case of “Pseudo-Linear” (Fig. 7.a) and the lowest efficiency achieved for the case of “Diagonal Quadratic” model, presented in Fig. 7.a). The set of specific variables includes “Gamma”, “Delta”, “Sigma”, “Mu”, etc. The matrix of correct membership defined and misclassification on Fig. 8 shows a total of 141 and 137 traffic samples with correctly defined membership in verification procedures, out of a total of 156 informative observations.



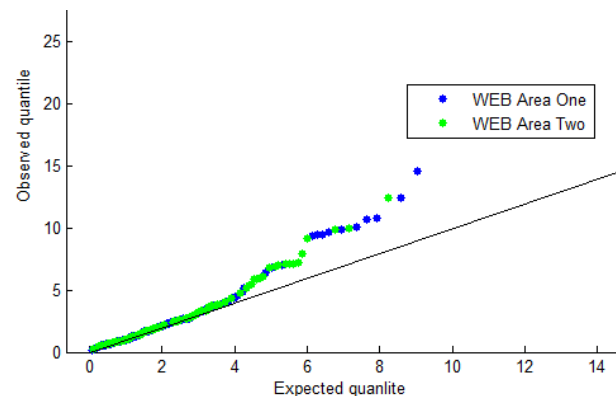
a)



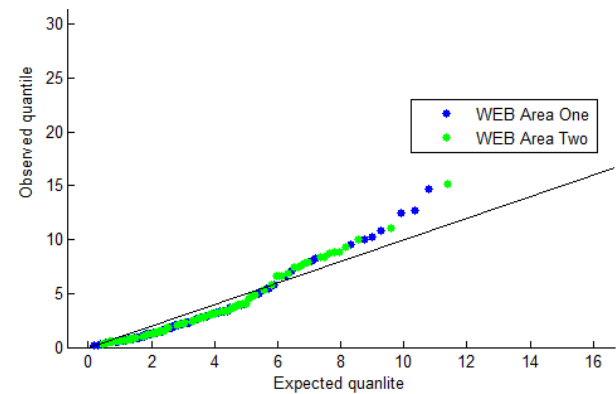
b)

Fig. 8. Confusion matrices in “Pseudo-Linear” and “Diagonal Quadratic” model assessment process.

In connection with confirming the correctness of the application of the analytical tool, “Quantile-Quantile” plots were constructed to compare two probability distributions by displaying and evaluating the behavior of “Observed” and “Executed” quantiles. The resulting Q-Q diagrams for the cases of “Pseudo-Linear” and “Diagonal Quadratic” discriminant models are shown in Fig. 9.



a)



b)

Fig. 9. Q-Q diagrams for “Pseudo-Linear” and “Diagonal Quadratic” discriminant model verification procedures.

For a significant share of statistical analyzing, the data sample possesses a "Gaussian distribution", which is a positive indication of the correctness of the use of the selected mathematical apparatus.

V. CONCLUSION

Effective diagnostics of network traffic with Machine Learning tools will significantly improve the efficiency of information services, Internet service providers and network operators. The information datasets analyzed covers complex metrics for registered traffic in relation to 200 companies for two geographic areas in the central part of the city of Chicago in active time zones 9.00 to 12 a.m. / 1.00 to 4.00 p.m. The total data is divided in a basic ratio of 2:1, respectively for training / testing procedures and evaluation through validation models for verification. The conducted research represents one of the main technical directions in this field. Future technical prospects for upgrading the scope of the considered issues can be divided into the following categories:

- Integrating classification and predictive analysis in terms of Cybersecurity management when ensuring access to electronic resources and services;
- Introduction of Design of experiment concept and non-linear minimization by optimization methods and algorithms related to complex performance indices of transmission media and traffic load evaluation of network servers, distribution units and system modules in communication and information systems.

ACKNOWLEDGMENT

The research was funded by Project "Quality of Service and Cybersecurity on Network Diagnostics in Communications by Artificial Intelligence" – Technical University of Gabrovo, Bulgaria.

REFERENCES

- [1] A. Shahraki, M. Abbasi, A. Taherkord and A. Jercut, "Active learning for network traffic classification: A technical study," IEEE Transactions on Cognitive Communications and Networking Journal, vol. 8, no. 1, p. 422+, October 2021. Available: DOI: [10.1109/TCCN.2021.3119062](https://doi.org/10.1109/TCCN.2021.3119062).
- [2] T. Vashishth, V. Sharma, B. Kumar and S. Chaudhary, "Artificial intelligence-enabled traffic optimization: A comprehensive survey," Industrial Engineering Journal, vol. 52, no. 5, p. 26+, May 2023.
- [3] A. Guo and C. Yuan, "Network intelligent control and traffic optimization based on SDN and artificial intelligence," Electronics Journal, vol. 10, no. 6, p. 2+, March 2021. Available: <https://doi.org/10.3390/electronics10060700>.
- [4] M. Latah and L. Toker, "Application of artificial intelligence to software defined networking: A survey," Indian Journal of Science and Technology, vol. 9, no. 46, p. 3+, November 2016. Available: DOI: [10.17485/ijst/2016/v9i44/89812](https://doi.org/10.17485/ijst/2016/v9i44/89812).
- [5] H. Shein, "Signal processing technology of mobile communication system based on artificial intelligence", Procedia Computer Science Journal, vol. 261, p. 1284+, December 2025. Available: <https://doi.org/10.1016/j.procs.2025.05.003>.
- [6] T. Singasani, M. Shaik, C. Gangajaliya, S. Ogety, V. B. Nallam and S. Katta, "AI-driven signal processing: Improving communication systems with machine learning-based noise reduction," in First International Conference on Radio Frequency Communications and Networks India, 2025, pp. 1-6.
- [7] Z. Bai, "Research on Application of Artificial intelligence in communication network," IOP Publishing Journal of Physics, vol. 2209, no. 1, p. 3+, February 2022. Available: DOI: [10.1088/1742-6596/2209/1/012014](https://doi.org/10.1088/1742-6596/2209/1/012014).
- [8] G. Fontanesi et al., "Artificial intelligence for satellite communication: A survey," IEEE Communications Surveys & Tutorials, vol. 28, no. 1, p. 1381+, February 2025. Available: DOI: [10.1109/COMST.2025.3534617](https://doi.org/10.1109/COMST.2025.3534617).
- [9] A. Thakur, "Artificial Intelligence (AI) in Information and Communication Technology (ICT): An Overview," International Journal of Research and Analysis in Science and Engineering, vol. 1, no. 3, p. 34+, May 2021.
- [10] K. Naseer Qureshi and T. Newe, Artificial Intelligence of Things: New Standards, Technologies and Communication Systems. NY: CRC Press Taylor & Francis Group, 2024.
- [11] K. Koufos, K. Haloju, M. Dianati, M. Higgins, J. Elmirghani, M. Imran and R. Tafazolli, "Trends in intelligent communication systems: Review of standards, major research projects, and identification of research gaps," MDPI Journal of Sensors and Actuator Networks, vol. 10, no. 4, p. 23+, October 2021. Available: <https://doi.org/10.3390/jsan10040060>.
- [12] Y. Mao, A. Pranolo, L. Hernandez, A. Wibawa and Z. Nuryana, "Artificial intelligence in mobile communication: A Survey," IOP Conference Series Journal: Materials Science and Engineering, vol. 1212, no. 1, p. 2+, January 2022. Available: DOI: [10.1088/1757-899X/1212/1/012046](https://doi.org/10.1088/1757-899X/1212/1/012046).

Two Decades of Baltian-Latgalian Electronic Dictionary

Ansis Ataols Bērziņš
Riga Technical College
Riga, Latvia
ansis@latnet.lv

Abstract — We would like to present the dictionary we have been compiling for two decades, as well as the electronic lexicographic system used to create it, which was specifically developed for this purpose twenty-three years ago. This is a good example of an almost-without-financing, long-term strategy for developing IT systems for language technology purposes, and it could be successfully used to create dictionaries for other endangered languages as well.

Keywords — dictionary, electronic, lexicography, language technology, endangered, less-resourced, Latvian, Latgalian, Baltian.

In 2003, the author created a new electronic system for the Baltic Latvian – Latgalian Latvian dictionary, which he began compiling in the late 1990s together with Armands Kociņš.

In slang, Baltic Latvian is simply called Latvian, and Latgalian Latvian is simply called Latgalian. However, this is not entirely correct, as both nations identified themselves as Latvians („latvieši“ in Baltic Latvian and „latviši“ in Latgalian Latvian). Therefore, we suggest using the terms Baltian and Latgalian instead when shorter forms are needed.

In 2004, the dictionary had 2,000 entries, in 2006 – 8,000, in 2011 – 14,000, in 2017 – 24,000, and now there are almost 28,000. In 2010, a public interface was created, and all these years it has been widely used by people interested in the Latgalian language. This entire job was done without any luck in financial support; we had just some small projects with budgets of a couple of hundred lats (Ls, LVL). The architecture of the dictionary from the very beginning was innovative – it was not just a translation dictionary, but a kind of integrated, universal dictionary that included information for the simultaneous development of translation, explanatory, terminological, dialectal, and other types of dictionaries, with the

possibility of their separate use afterwards. [7] In traditional „paper“ lexicography, the dream of a universal dictionary has been known at least for many decades.

Для теории лексикографии необходимо понятие максимальной лексической системы и понятие универсального словаря, в котором зафиксирована максимальная лексическая система.¹ [8]

It is recognised as merely a theoretical, idealistic and unrealisable construction. Objectively, due to the limitations of paper format – it is impossible to include all the information and maintain the readability of the text.

Универсальный словарь должен существовать в качестве лексикографического идеала в умах составителей словарей. Это цель, достижимая лишь в абстракции.² [4]

However, there are successful partial realisations of this concept, for example, The Big Chinese-Russian Dictionary:

БКРС занимает особое место среди двуязычных китайско-русских словарей. Возможно даже, что среди двуязычных словарей он вообще не имеет аналогов. Как лингвистический словарь он вообрал в себя различные аспекты китайского языка, сведения о которых обычно выносятся в отдельные словари — грамматические, толковые, фразеологические, диалектные, исторические, этимологические. Вместе с тем он расширил рамки лингвистического словаря до энциклопедического, став энциклопедией культуры, общественных отношений, духовного облика Китая и даже местного колорита.³ [9]

Electronic dictionaries are not limited in their filtering capabilities, which is the main problem for paper dictionaries when dealing with large volumes of information, especially across different types of it. Thus, it is possible to collect and include all information for all dictionary types covered by the „umbrella“ of universality,

¹ For the theory of lexicography, the concept of a maximal lexical system and the concept of a universal dictionary in which the maximal lexical system is fixed are necessary.

² A universal dictionary must exist as a lexicographic ideal in the minds of dictionary compilers. This is a goal achievable only in the abstract.

³ The BCRS occupies a special place among bilingual Chinese-Russian dictionaries. It may even be unique among all bilingual dictionaries. As a linguistic

dictionary, it encompasses various aspects of the Chinese language, information about which is usually confined to separate dictionaries – grammar, explanatory, phraseological, dialectal, historical, etymological. At the same time, it expanded the scope of the linguistic dictionary to become an encyclopaedic one, becoming an encyclopaedia of culture, social relations, the spiritual makeup of China, and even local flavor.

but display only partial information in a filtered format for a lexicographic subtype that best suits users' needs.

Now that our electronic dictionary has reached the required level and volume, it is time to edit and publish the

paper version too – this is the final step we plan to take using our electronic system in order to, we hope, preserve this edition of the dictionary for centuries.

acotāj[s] [•ac`uotā̃ js...tā ja] *subst.* (*dārz.*) čepituojs/s, -a [•č`ēp`^ēit`uojs`...t`uoj`ā] [Labot](#)
acotnīs [•ac`uotnīs] *subst.* (*dārz.*) čepjamaš auguojis [•čēp`ēj`ām`ais`•^aug`uojs`] [Labot](#)
acot[s]^a [•ac`uots...•ac`uota] *partic.* čepit/s, -a [•čēp`^ēic`...p`^ēita]; a. augš — čepits auguojis
acot[s]^b [•ac`uots...•ac`uota] *adj.* -> acains [Labot](#)
ac[s] *subst.* 1. acs [ačs] (*vsk. ģen. un dsk. nom.* acs [ačs]; *dem.* acēna); **zaudēt ~u gaismu** — palikt bez acu spūdruma; **viņš zaudējis ~u gaismu** — jam aptymsa acs; **labas ~is (gaišas ~is)** — spūdrys acs (loba redzeiba); **vecamtevam vēl gaišas ~is** — vacikam vēl spūdrys acs (vaciks vēl labi redz); **~s zīlīte** — acs zierneits (acs leleite); **~s lēca anat.** — acs lāca; **~s dobums anat.** — ocudūbs [...b`'s`]; **~s ābols anat.** — acs uobeljs; **~u slimības** — acu vainis; **~u ārsts** — acu uorsts; **~u aizsargs** — ocusorgs; (*kāda*) **~u priekšā** — (*kuo*) acis; **visu ~u priekšā** — vysu acis; **nolasīt (kādam) no ~im atbildi** — puorskaiteit (*kuo naviņ*) acis atsacejumu; **skatīties (kādam) acīs** — vērtīs (*kam*) acis; **~u pilieni** — acu lasis; **~is krīt ciet (~is līp ciet)** — acs lypst kūpā (acs koč ar skalenim sprīd); **blisināt ~is sar.** — bulynuot acs; **pievērt ~is tiešā un pārn. noz.** — danierkšt acs; **raibs sametās (viss nīrbēja; melns metās; zils) gar ~im tiešā un pārn. noz.** — mygla viņ apsamete ap acim; **~is lielas kā pogas (~is platas kā pogas; ~is lielas kā šķīvji; ~is platas kā spoles)** — acs kai opūgam (plotys acs kai opūgam); **~is kļuva sarkanās kā trusim (kā vēzim, kā vērsim)** — acs apsorka kai ar suoli pībārtys; **pats savām ~im redzēju** — pats ar sovom acim redzēju; 2. (*kartupeļa*) acēna; 3. (*gredzena*) acēna; 4. (*adatas, tīkla*) acs; 5. (*adīkļa*) kalpeņš; 6. (*kāršu spēlē*) acs;
 ◇ **ar ~im vienmēr var apēst vairāk (ar ~im varētu apēst vēl)** — progoreigys acs vys ēst grib; **viņš ~is neko sliktu nesaka, bet aiz muguras aprunā** — acis tu jam lobs, a aiz acu nalobs (acis engeļs, aiz acu valns); **~is darba izbījās, rokas darba nebījās** — actenis apsabeist, rūcenis padora (acs apsabeist, a rūkys padora); **uzmest ~i (uzmest ~is)** — puorskrīt ar acim; **lūdzu, uzmet ~i, vai viss kārtībā!** — lyudzams puorskrīt ar acim, ci vyss parādā!; **no pirmā ~u uzmetiena** — nu pyrmuo pasavīerīņa; **viņš viņā iemīlējās no pirmā ~u uzmetiena** — jis jū imīļova nu pyrmuo pasavīerīņa; **krist ~is** — svīstīs acis; **nolaidība krīt ~is** — apsalaisšona svīzās acis; **dot (ko) par skaistām ~im (tāpat vien, bez nopelniem)** — dūt (*kū*) par skaistu vaigu; **par skaistām ~im ordeni nedod** — par skaistu vaigu ordīņa nadūd; **redzams ar neapbruņotu ~i** — ar prostom acim monoms; **kolagēnšķiedras ar neapbruņotu ~i nav redzamas** — kolagena šķīznys ar prostom acim namonomys; **bāzt ~is (bāzt sejā; mest acīs; mest sejā)** — lepēt acīs (īgryust acis; svīst kai ar suoli acis) [Labot](#)
 Piezīmes:
 Piezīmes: - **acs** — acēna, aceite, das Auge (-s, -n).. / **acs** (adeiklam), die Masche (-, -n)..(.).. **acs** (kartom, kauleņam), **acs** (odotas), das Ōhr (-/e/s, -e), **acs** (teiklam), die Masche (-, -n).., **acēna**
 psl.) — AK
 Piezīmes: - Ar viņu **aci** veras menesnika, bet ar utru uz sabra dorza... - (Kristopa Brema „Ceļojums pa Latgolu”, [Preili] : Jasmuiža, 1992, 7 psl.) - EM
 Piezīmes: - ...kad jis pimdz kreisu **aci**, tod zyni, ka te Joņa k-gs skrin pa gaisu. - (Kristopa Brema „Ceļojums pa Latgolu”, [Preili] : Jasmuiža, 1992, 4 psl.) - EM
 Piezīmes: - Ar viņu rūku ēst dūd, ar ūtru lizeikas kōtu dur **acīs**. - ("Mōras Zeme" // "Rēzeknes Vēstis", 17.06.2010) - AK

Fig. 1. An example of „as-paper-dictionary“ printout of the dictionary.

Electronic development of dictionaries opens up new possibilities for developers and makes non-topical classical lexicographic perceptions.

However, it adds risks of inappropriate quality too:

Очертания современной лексикографии существенно изменились в связи с внедрением компьютерных технологий: с одной стороны, появились реальные возможности осуществления в обозримые сроки масштабных лексикографических проектов, с другой — расширилось пространство для деятельности компиляторов.⁴ [5]

In our dictionary and development system we strive to keep all the values of paper dictionaries, and just to add advantages of electronic ones.

While dictionaries were developed „on paper“, the main question was „what to include and what not to include?“. The balance between wishes and possibilities, between interestingness and perceptibility of information, between knowledge and space was the main lexicographical challenge.

⁴ The contours of modern lexicography have changed significantly due to the introduction of computer technology: on the one hand, real opportunities have emerged for the implementation of large-scale lexicographic projects within a

foreseeable timeframe; on the other, the scope for the work of compilers has expanded.

Vārds: **ēna** (atrasts)

☐ Homonīms vai homogrāfs: Atdalītājs aiz burta Nr.: Saīsinājumi:

Nozīmju skaits: Izruna: Defise: Paskaidrojums: S.dz.sāk.: S.dz.gal.: S.dz.izr.:

1.

☐ Skatīt vārdu, homogrāfu, nozīmi: Saīsinājumi: Gram. forma:

Mainīt nozīmes numuru: Tulkojumu skaits: Piemēru skaits: Paskaidrojums: Konteksts:

☐ Tulkojums: Saīsinājumi: Locīšana: Defise: S.dz.sāk.: S.dz.gal.: S.dz.izr.:

Paskaidrojums pirms: Paskaidrojums aiz: Izruna:

☐ Tulkojums: Saīsinājumi: Locīšana: Defise: S.dz.sāk.: S.dz.gal.: S.dz.izr.:

Paskaidrojums pirms: Paskaidrojums aiz: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

2.

☐ Skatīt vārdu, homogrāfu, nozīmi: Saīsinājumi: Gram. forma:

Mainīt nozīmes numuru: Tulkojumu skaits: Piemēru skaits: Paskaidrojums: Konteksts:

☐ Tulkojums: Saīsinājumi: Locīšana: Defise: S.dz.sāk.: S.dz.gal.: S.dz.izr.:

Paskaidrojums pirms: Paskaidrojums aiz: Izruna:

☐ Tulkojums: Saīsinājumi: Locīšana: Defise: S.dz.sāk.: S.dz.gal.: S.dz.izr.:

Paskaidrojums pirms: Paskaidrojums aiz: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

☐ Piemērs pirms: Piemērs aiz: Saīsinājums: Paskaidrojumi: Izruna:

Piezīmes:

- ..pasargos nakti susatiwi (ciēn) nu kō nibiēš.., tyūlēn godoj un rur
 - Susatiwi parodiejot Sowu, kurs nikniņ iznika. - ("Inflantuziemies t:
 - Kae rīcās nēraukēt) (Susatiwē) - (tairu mēiklā) - ("Tairas dīcēm t:
 < >

Nosūtīt No jauna Homonīmu/homogrāfu skaits: Stāvoklis: Pārjaunot veidlapu

ēn|a subst. 1. (tumšs atspīdums) susātvīs; susāts poēt.; **koka ē.** — kūka susātvīs; **cilvēka ē.** — cylvāka susātvīs; **mest ~u t. un pār.** — mest susātvī; **gulēt ~ā** — gulēt susātvī;
 < **palikt (kāda) ~ā** — palikt (kuo) susātvī; **baidīties no savas ~as** — beifis sova susātvī; **acu ~as** — ocu susātvī; **~u valstība** — susātvī kieneste
 2. (vieta, kur var patverties no saules) pakrieslīs; krieslīs poēt.; **koka ē.** — kūka pakrieslīs; **no saules patverties ~ā** — nu saulis globuotīs pakrieslī; **vairums augu ~ā neaug** — lelums augu pakrieslī naaug

Fig. 2. An example of the interface for editing one entry of the dictionary..

Electronic systems give us the ability to filter in real time. This means we can collect all available information without any disturbance of further work in case of forward-looking design of the dictionary structure and the architecture of the development software too. This fundamentally changes the basic principles of dictionary creation and deserves extensive discussion and analysis. Moreover, this means that the main classification criteria used for „paper“ dictionaries become secondary when creating a „universal“ electronic dictionary: all of them can be used as filtering criteria (instead of creating criteria): the density of entries can cover both general and narrow, as well as special lexis (regional and social dialects, jargons and slangs, archaisms), monolingual dictionary can be combined with a bilingual (or even multilingual) one, lexical data – with encyclopaedic data, diachronic (dynamic) data – with synchronic (static), normative – with referential, data for general use – with specialised. Arrangements can be defined freely depending on users' needs, including alphabetical and semantic ones. Simultaneous development of translational, explanatory, terminological, dialectal, phraseological and other types of dictionaries with a possibility of separate usage of them afterwards from one side makes the process more rational, as it allows all the information to be stored in the right place at the same time. On the other hand, it makes the system more cumbersome, and the design process significantly more complex. How can such a „universal“ dictionary and its development system be created? What should be considered? Certainly, by universality we mean not only the type of dictionary content, but also its technical meaning: a single dictionary should meet the needs of both modern electronic (both offline and online) dictionaries and traditional „paper“ dictionaries—it should be capable of automated printing and proper publication. We felt the idea of universality and integrity of dictionary from the very beginning of our work on it, however it was formalised and formulated just in [7] – what it should contain, what should be included, what kinds of classic „paper“ dictionaries it should cover etc. Off course, there is nothing absolute in this world, and universality does not mean that it covers all possible dictionary variations, but only a fairly large part of them. For now, if we look at Shcherba's list of lexicographical contradictions – he determined the impossibility of combining the terms of both contradictions in a single dictionary – we will see that we have combined 5 of the 6 pairs (with the exception of the distinction between the standard and the ideological; however, if necessary, we can also add an option of ideological structuring too).

Одним из первых вопросов лексикографии является, конечно, вопрос о различных типах словарей. Он имеет непосредственное практическое значение и эмпирически всегда как-то решался и решается. Между тем в основе его лежит ряд теоретических противопоставлений, которые и необходимо вскрыть.

1. Противоположение первое: словарь академического типа — словарь-справочник ...
2. Противоположение второе: энциклопедический словарь — общий словарь ...
3. Противоположение третье: thesaurus — обычный (толковый или переводный) словарь ...
4. Противоположение четвертое: обычный (толковый или переводный) словарь — идеологический словарь ...
5. Противоположение пятое: толковый словарь — переводный словарь ...
6. Противоположение шестое: неисторический словарь — исторический словарь ...⁵ [3]

Two decades ago, we made such a development system, and all this time we've been slowly but steadily filling it with linguistic data (of all types suitable for lexicographical purposes and from all sources available for us).

We began explaining the idea behind our lexicographical system in [4] and, as we previously wrote, have been formulated a conceptual generalisation that can be used as a kind of manual for creating other integrated / universal dictionaries in [7]. We published several more examples of what entries in our dictionary look like in [1]. The dictionary is also available online. [6] We are currently continuing to provide updates on the progress of our dictionary development and are also considering integrating other natural language processing methods (for example, based in machine learning and deep learning) both for collecting language usage examples for the dictionary and for generating language resources (e.g., parallel corpora, machine translation models etc.) with the help of the dictionary.

Now it's time to take the next step and to prepare it for print. The system supports automatic output in a look of paper dictionary from the very beginning. This means that even the data structure was created specifically to cover almost any paper dictionary (we analysed a lot of them during the design stage). Therefore, the preparation for publication does not mean adaptation, but just a usual editorial work of fully preparing the content, editing, and correcting mistakes. In any case, this is too much of a workload for two researchers without organisational background and financial support. Thus, we are open to proposals from institutions interested in: 1) publishing the Baltian-Latgalian (and in future probably Latgalian-Baltian too) dictionary; 2) to prepare and publish other dictionaries.

REFERENCES

- [1] Bērziņš A.A. Latgaliešu terminoloģijas izstrāde // Latviešu terminoloģija simts gados. LNB zinātniskie raksti. 6. (XXVI) sējums. Rīga: Latvijas Nacionālā bibliotēka, 2020.
- [2] Берзінь А.У. Электронная сiстэма распрацоўкі латышка-латгальскага слоўніка // Язык и межкультурные коммуникации. Минск: БГПУ, 2011.
3. Contrast three: thesaurus vs. standard (explanatory or translation) dictionary ...
4. Contrast four: standard (explanatory or translation) dictionary vs. ideological dictionary ...
5. Contrast five: explanatory dictionary vs. translation dictionary ...
6. Contrast six: non-historical dictionary vs. historical dictionary ...

⁵ One of the most important questions in lexicography is, of course, the question of the different types of dictionaries. It has immediate practical significance and has always been and continues to be addressed empirically. However, at its core lies a series of theoretical contrasts that need to be explored.

1. Contrast one: academic dictionary vs. reference dictionary ...

2. Contrast two: encyclopedic dictionary vs. general dictionary ...

- [3] Щерба Л.В. Языковая система и речевая деятельность. Москва: Наука, 1974.
- [4] Дубичинский В.В. Теоретическая и практическая лексикография. Вена-Харьков: Gesellschaft zur Förderung slawistischer Studien, 1998.
- [5] Козырев В.А., Черняк В.Д. Современные ориентации отечественной лексикографии // Вопросы лексикографии. № 1 (5). Томск: Томский государственный университет, 2014.
- [6] Bierzeņš A.A., Kūceņš A. Baļtīšu-latgaļīšu vuordineica. <http://vuordineica.lv/> [Accessed 16.IV.2026]
- [7] ბერზინი ა.ა. უნივერსალური ლექსიკონის კონცეფცია / Conception of the Integrated Dictionary // II საერთაშორისო სიმპოზიუმი ლექსიკოგრაფიაში / II International Symposium in Lexicography. ბათუმში / Batumi, 2012.
- [8] Денисов П.Н. Системность и связанность в лексике и система словарей // Проблематика определений терминов в словарях разных типов. Ленинград: Наука, 1976.
- [9] Стабуrowa Е.Ю. Большой китайско-русский словарь: к 40-летней годовщине // Российское китаеведение. № 3(4). Москва: Институт Китая и современной Азии РАН, 2023.

Real-Time Network Traffic Capture and Analysis Using a Deep Neural Network

Angela R. Borisova

Computer Systems and Technologies Department
"Vasil Levski" National Military University
Shumen, Bulgaria
arborisova@nvu.bg

Krasimir Slavyanov

Computer Systems and Technologies Department
"Vasil Levski" National Military University
Shumen, Bulgaria
k.o.slavyanov@gmail.com

Abstract—Nowadays, computer networks generate large and complex data sets, which leads to problems related to the detection of new, modified threats. Classic Intrusion Detection Systems – IDS, based on static rules and signatures, have difficulty identifying masked - as legitimate or previously unseen malicious activities. The challenge they face is reverse shell attacks, in which the attacker establishes a seemingly reliable connection with the victim. This study presents an approach aimed at solving a problem related to the cybersecurity of computer systems and networks. This is done by building, training, and testing the effectiveness of deep neural architectures for recognizing illegitimate reverse shell packets passing through a computer network in a controlled and real-world environment.

The simulation of the attacks is carried out in a protected environment – Oracle Virtual Box. The interception of network packets in real time is carried out using a software tool written in the Python programming language. Packet sniffing itself is performed both in the virtual environment and in the real environment. The sniffer script extracts significant sets of characteristics from network packets, such as packet size, protocols used, ports, TCP flags, IP addresses - of the source (attacker) and the recipient (victim), and others. The current report compares several deep neural networks, namely One-dimensional convolution neural network/1D CNN, Long Short-Term Memory/LSTM and Autoencoder. As 1D CNN, it extracts local dependencies between network packet features for traffic classification. LSTM models capture temporal dependencies and sequences from network data, and autoencoders reconstruct normal network behavior patterns. The results of the experiments reveal the ability of deep neural networks to correctly model the behavior of network traffic and ultimately increase the recognition of compromised data. The proposed approach offers the opportunity to further automate the processes of detection and monitoring of computer systems, which in turn would lead to the protection of network infrastructure in modern dynamic environments.

Keywords — *LSTM, 1D CNN, Autoencoder, reverse shell attacks*

I. INTRODUCTION

The continuous development of network technologies and the rapidly increasing complexity of cyber threats

make network security an extremely important component in communication and information systems. Classic machine learning algorithms and traditional intrusion detection systems (IDS - which are inherently signature-based) are unable to cope with the constantly changing modern cyberattacks, especially those in real-time conditions - known as unknown or zero-day.

Deep learning algorithms have the potential to overcome cyber challenges by extracting complex dependencies from large volumes of network data. Deep neural architectures such as Long Short-Term Memory (LSTM), convolutional neural networks (CNN), and autoencoders, are a good option due to their properties. Autoencoders capture illegitimate network packets thanks to their unsupervised learning nature, which helps them learn the normal behavior of network data flows. Long Short-Term Memory is capable of modeling temporal dependencies in data sequences, and convolutional neural networks capture spatial dependencies between network traffic characteristics.

To date, most studies have been based on pre-collected (offline) datasets and do not adequately address latency in the detection of cyberattacks. Since network traffic in real-world conditions is continuous and massive, it requires processing with minimal delay. Therefore, network anomaly detection models must be automated and capable of operating in a streaming environment in order to respond instantly [9] to a cyber incident [10].

This research paper presents an approach for capturing and analyzing network traffic both in controlled conditions and in real time, by leveraging the capabilities of three types of deep neural architectures. It compares the effectiveness of LSTM, 1D CNN, and autoencoder networks in detecting various types of network behavior—normal traffic, reverse shell attacks, and unknown anomalies.

The article is structured as follows: Section 2 – describes existing research in the field. Section 3 – describes the methodology and architecture of the model. Section 4 – describes the results of the study and the subsequent analysis. Section 5 – describes the conclusions

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.112>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

from the work performed and provides guidelines for future work.

II. OVERVIEW OF EXISTING SOLUTIONS

Article [1] proposes a deep learning-based **hybrid model** that combines **LSTM** and **CNN**. The main idea of the proposed hybrid architecture, called Attention-CNN-LSTM, is that an attention layer is added, aiming to improve accuracy by reducing noise pollution. For training and testing the neural architecture, the following datasets are used: NSL-KDD and Bot-IoT (they are realistic and publicly available datasets collected in a controlled laboratory environment).

Attention-CNN-LSTM achieves high accuracy of 94.8% (experiment conducted on NSL-KDD dataset) and 97.5% (experiment conducted on Bot-IoT dataset) and low false positive rate. However, the study is based on previously collected (offline) network data, which is outdated and does not contain encrypted traffic. Furthermore, the proposed model does not address the challenges associated with processing network packets in a streaming environment.

In the paper [2], a **hybrid model** for anomaly detection in photovoltaic systems is proposed, which combines a convolutional neural network and an autoencoder - **CNN-Autoencoder**. Although the paper is not directly related to network traffic analysis, it considers deep-structured neural architectures for recognizing normal and abnormal behavior, which is conceptually similar to the approaches in intrusion detection systems. The dataset used is GPVS-Faults. The GPVS-Faults data represent real measurements collected in advance by a photovoltaic system emulator via sensors.

The results show that the proposed CNN-Autoencoder hybrid architecture significantly improves the diagnostic accuracy compared to standard CNN models, reaching 98.84% accuracy. In addition, a significant reduction in the false alarm rate is observed. However, despite the high performance, the method is validated mainly on offline data collected from an emulator system, which limits its direct applicability in real dynamic environments.

The proposed neural architecture for intrusion detection in [3] combines two levels of deep learning, namely **Hybrid Autoencoder (HAE)** and **Hybrid Residual LSTM-CNN network (HRL)**. The datasets used in the study are previously collected and publicly available, namely: NSL-KDD, UNSW-NB15 and CICIDS-2018.

The analysis of the reviewed research shows that the model training is stabilized by using residual connections. However, the improvement in accuracy compared to classical models based on LSTM and CNN is relatively limited and is usually within 1–3%. The proposed combined model is characterized by increased architectural complexity, which leads to the need for significant computational resources and a higher implementation cost. In addition, there is a partial overlap of functionalities between the individual components – the autoencoder compresses and represents the input space,

while the CNN performs feature extraction, with both modules implementing different aspects of data representation. Additionally, the increased complexity of the model creates prerequisites for the occurrence of overfitting. Furthermore, the experimental evaluation was performed in an offline environment, which limits the possibility of evaluating the behavior of the model under real network traffic.

In the paper [4], a comparative analysis is made between the efficiency and accuracy of **CNN + Bidirectional LSTM (BiLSTM)** and **machine learning models**. The datasets involved in the study are: NSL-KDD, UNSW-NB15.

The experimental results show that deep neural models achieve higher accuracy (98.96% – 99.78%) compared to classical machine learning approaches (95% – 98%) in intrusion detection tasks. However, it should be noted that the evaluation was performed on static data in an offline environment, which limits the direct applicability of the results to real-world conditions.

Paper [5] addresses the security issue in software-defined networking, SDN, emphasizing that the centralization and programmability of the network create new vulnerabilities. The authors propose the application of advanced deep-structured models - a **hybrid CNN-LSTM** model and a **Transformer encoder** model - for attack detection, focusing on SDN security. The dataset used is InSDN. This dataset was previously collected in a controlled laboratory environment and contains both normal traffic and simulated attacks.

According to the research, the accuracy of CNN-LSTM, relative to the number of input features, is in the range of 98.20% - 99.01%, and the accuracy of Transformer encoder, again relative to the number of input features, is in the range of 98.50% - 99.02%. After merging rare classes and applying binary classification, the accuracy reaches 99.19%. However, the results were obtained on controlled data and do not guarantee the same efficiency in a real environment.

Paper [6] presents a hybrid architecture - **Autoencoder-LSTM/BiLSTM** for intrusion detection. Initially, the autoencoder is used to detect anomalies by comparing the input data and its reconstruction error. Then, the LSTM network classifies the suspicious flows by analyzing their time sequence. The dataset used is NSL-KDD.

The Autoencoder-LSTM model shows improvement over classical ML methods, but the achieved accuracy – 89% and the high false alarm rate – 11% make it less reliable than modern deep-structured anomaly detection architectures. The results are valid mainly for offline controlled conditions and do not fully reflect the behavior in real network environments.

Paper [7] presents an overview of **CNN-based approaches** for network intrusion detection, analyzing different architectures, feature extraction methods, and datasets used. The main conclusion is that CNN models are effective in automatically extracting features from network traffic, but their use alone is limited in terms of

modeling temporal dependencies. Therefore, hybrid architectures combining CNN with other deep models show better overall performance. The study itself was conducted in a controlled environment and was not tested in a real-world setting.

Article [8] proposes an **LSTM** model optimized with **metaheuristic algorithms** for detecting network attacks. The aim of the study is to automatically tune the hyperparameters of LSTM – number of neurons, layers, etc. The neural model was trained and tested using 3 standard datasets: NSL-KDD, CICIDS2017 and BoT-IoT.

After the experiments, it was found that the best result is achieved by SSA-LSTM (LSTM + Salp Swarm Optimization). SSA-LSTM reaches an accuracy of approximately 99%, and it also has the lowest false positive rate. LSTM is a good option for detecting intrusions, but on its own it is not optimal. The research in the article was conducted in an offline environment.

Contrary to the research conducted and the good results of hybrid models, three separate, non-combined deep neural networks will be examined and an attempt will be made to prove that with appropriate model design, they would give almost excellent results in detecting anomalies in computer networks, both in a controlled and real environments.

III. MATERIALS AND METHODS

To fulfill the task set in this report, namely the collection and analysis of network data in real time, three neural network multilevel models – LSTM, One-Dimensional Convolutional Neural Network (1D CNN) and Autoencoder – have been developed, trained and tested for extracting features from network traffic. The three models model network communication through statistical, behavioral, and semantic representations. In order to describe the temporal and statistical characteristics of network traffic, parameters are used that describe the dynamics of the quantitative properties of the traffic, namely: length of a specific packet, number of packets per second, interval between consecutive packets, indicators of burst behavior - many packets for a very short time interval, throughput in bytes per second. To describe the behavioral characteristics of the network, the dynamics and abnormal behaviors in the network data are monitored, such as: small packet indicator, retransmission detection, keep-alive and zero-window states, repeating ACK events, consistency of the communication direction - describing the degree of consistency in the alternation of incoming and outgoing packets within a flow. The semantics of the network is represented by examining the meaning of the traffic behavior, using shell/command pattern recognition.

For the purposes of the experiment, the following are used: Python 3.13 programming language, PyCharm 2025.2.1 integrated script development environment, Oracle VirtualBox virtual environment, Kali Linux machine, Windows Server 2025 machine and Wireshark 4.6.4 software. A comprehensive system for identifying normal and abnormal network behavior is created using Python programming language and PyCharm development environment. Reverse shell type network traffic is

simulated in a controlled, virtual Oracle VirtualBox environment, using a Kali Linux machine - playing the role of an attacker and a Windows Server 2025 machine - playing the role of a victim. Network data is collected using the Wireshark platform. To make the three neural networks used equal, they use a single pipeline architecture based on flow-aware segmentation and time windows of network traffic. Each sequence of packets represents a local time segment of network traffic, on which feature extraction is performed with a unified set of 60 features. Network flows are built based on a five-element identifier, including the sender's IP address, sender's port, recipient's IP address, recipient's port, TCP/UDP protocol. The data is organized into sliding windows of length 5 and step 1, which allows capturing local time dependencies in the traffic. To prevent mixing of unrelated sessions and detect intermittent or intermittent attacks, a time threshold of 30 seconds is introduced in all three models. Sequence labeling is based on majority voting, assuming that a sequence belongs to an attack class if more than 30% of the packets it contains are malicious. This ensures consistency between supervised 1D CNN and LSTM models and the unsupervised autoencoder.

There are three classes involved in the study, namely: two main classes - a normal traffic class and a reverse shell attack class, and one additional class called Unknown - if the network data is unknown to the models.

Again, to ensure that the networks used are equal, training is performed by setting the same hyperparameters: Adam optimizer, learning rate 0.0005, batch size 64, L2 regularization $1e-4$, and up to 150 epochs. To prevent overtraining, techniques such as: L2 regularization, learning rate reduction at standstill, early stopping, and dropout (0.3-0.5) are used. To balance the distribution of classes over training, validation, and testing in LSTM and 1D CNN, class weights and Focal Loss with parameters $\gamma = 2.0$, $\alpha = 0.25$ are used.

The data set used to train the three networks is the same. It is collected both in a controlled virtual environment and in a real one. Its size is approximately 44,000 packets. The raw data is converted to csv format and subsequently labeled with appropriate labels (for normal traffic – BenignTraffic, for reverse shell attack – RevShellAttack). Each record in comma separated value format contains sender information, recipient information, time between two consecutive packets within a flow, protocol, length of a specific packet, and a text field with additional metadata – TCP flags, TCP window size, HTTP, DNS, TLS handshake, shell commands, and more. To be brought into a single numerical standard, the data is normalized using StandardScaler. Categorical data (text data) is processed using label encoding (to convert labels to numerical format) and one-hot encoding (to convert protocol data to numerical format).

To prevent information leakage, data splitting is done at the data stream level, not at the individual packet level. Data for LSTM, 1D CNN networks is split as follows: 80% for training – normal traffic + recursive attacks, 10% for validation – normal traffic + recursive attacks, and 10% for testing – normal traffic + recursive attacks. In the case of the autoencoder, due to its nature of unsupervised learning,

the data is divided as follows: 80% for training - only data from normal traffic, 10% for validation of data from normal traffic and 50% for validation of data from reverse shell attacks, and 10% for testing data from normal traffic and 50% for testing data from reverse shell attacks.

The architectures of the three main deep neural networks look like this:

1. 1D CNN model architecture:

- input layer with the form: (sequence_length, num_features)
- first convolutional layer with dilation 1 and 32 neurons;
 - Batch normalization;
 - introducing nonlinearity through the Swish activation function;
 - dropout layer – 0.3 for regularization;
 - second convolutional layer with dilation 2 and 64 neurons;
 - Batch normalization;
 - introducing nonlinearity through the Swish activation function;
 - max pooling with a window size of 2;
 - dropout layer – 0.4 for regularization;
 - global average pooling;
 - fully connected layer with L2 regularization;
 - Batch normalization;
 - introducing nonlinearity through the Swish activation function;
 - Softmax output layer for binary classification.

2. LSTM model architecture:

- input layer with the form: (sequence_length, num_features)
- first Bidirectional LSTM layer with 64 neurons and L2 regularization – processing sequences in both directions, capturing local and medium-term dependencies;
 - Batch normalization;
 - dropout layer - 0.3 for regularization;
- second Bidirectional LSTM layer with 32 neurons and L2 regularization;
 - Batch normalization;
 - dropout layer - 0.4 for regularization;
 - fully connected layer with L2 regularization;
 - Batch normalization;
 - introducing nonlinearity through the Swish activation function;
 - dropout layer – 0.5 for regularization;
 - output Softmax layer for binary classification.

3. Autoencoder model architecture:

- input layer with the form: (sequence_length, num_features)
- Encoder:*
 - first convolutional layer in the encoding part with 64 neurons and L2 regularization;
 - Batch normalization;
 - introducing nonlinearity through the Swish activation function;
 - dropout layer - 0.3 for regularization;
 - second convolutional layer in the encoding part with 32 neurons and L2 regularization;

- Batch normalization;
- introducing nonlinearity through the Swish activation function;

- dropout layer - 0.4 for regularization;
- flatten layer and L2 regularization.

Decoder:

- first fully connected layer and L2 regularization;
- dropout layer - 0.4 for regularization;
- second fully connected layer and L2 regularization;
- reshape layer;
- dropout layer - 0.3 for regularization;
- first convolutional layer in the decoding part with 64 neurons and L2 regularization;
- Batch normalization;
- introduction of nonlinearity through the Swish activation function;
- second, reconstructing convolutional layer in the decoding part with 64 neurons and L2 regularization.

What distinguishes the three neural networks built in this study from most models used in practice for detecting malicious packets is the use of L2 regularization, Swish activation function, and convolutional layers with dilation.

In the framework of this study, experiments were conducted to collect, monitor and analyze the behavior of network traffic using sniffer scripts based on LSTM, 1D CNN and Autoencoder models. The study was carried out simultaneously, both in controlled conditions, through statically configured network parameters, and in real conditions, through dynamic IP address allocation. The metrics for evaluating the performance of the convolutional neural network, LSTM and autoencoder networks are: accuracy, precision, recall, F1-score, ROC-AUC and Confusion Matrix.

IV. RESULTS AND DISCUSSION

For the purposes of this report, experiments were conducted on network data recognition in a controlled and real-world environment. The Long Short-Term Memory, Convolutional Neural Network, and Autoencoder sniffers showed really good results – Table 1 and Fig. 1. – Fig. 9. It can be seen that each model processes between 7650 and 8565 network packets, generating approximately 6000 classification sequences. As far as possible, a balanced data set was collected to ensure unbiased evaluation of the models. Temporal LSTM models achieve 99.95% accuracy, with only 3 classified as Unknown, real recursive packet sequences. Spatial 1D CNN methods achieve 99.92% accuracy, with 5 uncertain detections, 3 of which are real recursive attacks and 2 of which are real normal traffic. The autoencoder, despite its unsupervised nature during training, achieves 100% accuracy, and proves to be an excellent solution for scenarios involving zero-day attacks. All three deep neural architectures achieve amazing ROC-AUC results – 1.000, indicating perfect discrimination between normal and malicious traffic. The ROC curves show that the models achieve 100% true positive rate, 0% false positive rate for LSTM and autoencoder. For 1D CNN, due to the negligible false positive rate of 0.07%, the ROC curve returns a value of 1.000 again.

TABLE 1 SUMMARY OF PERFORMANCE INDICATORS OF DEEP NEURAL MODELS – LSTM, CNN, AUTOENCODER

Model	Packets	Sequences	Benign Traffic	RevShell Attack	Unknown	Accuracy	Precision	Recall	F1-score	AUC
LSTM	8565	6049	2919	3130	3	99.95%	100%	99.90%	99.95%	1.000
1D CNN	7650	6039	2910	3129	5	99.92%	99.94%	99.90%	99.92%	1.000
Autoencoder	8180	6033	2903	3130	0	100%	100%	100%	100%	1.000

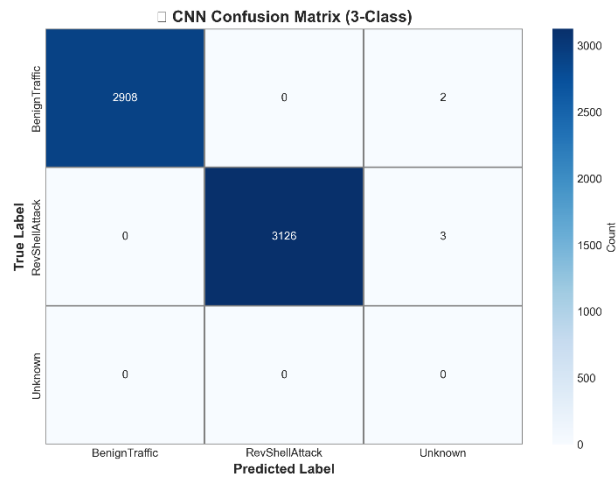


Fig. 1. Confusion matrix results in 1D CONVOLUTIONAL NEURAL NETWORK.

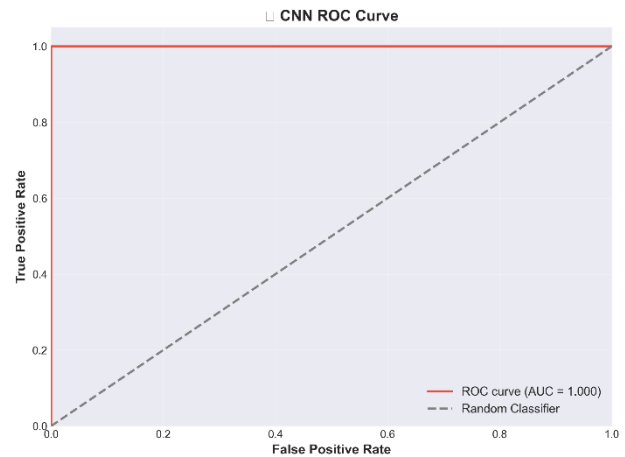


Fig. 3. 1D CONVOLUTIONAL NEURAL NETWORK performance evaluation via Receiver Operating Characteristics

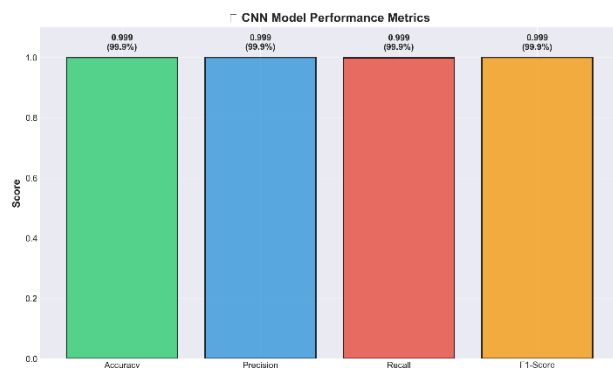


Fig. 2. Accuracy, precision, recall and F1-score of a 1D CONVOLUTIONAL NEURAL NETWORK.

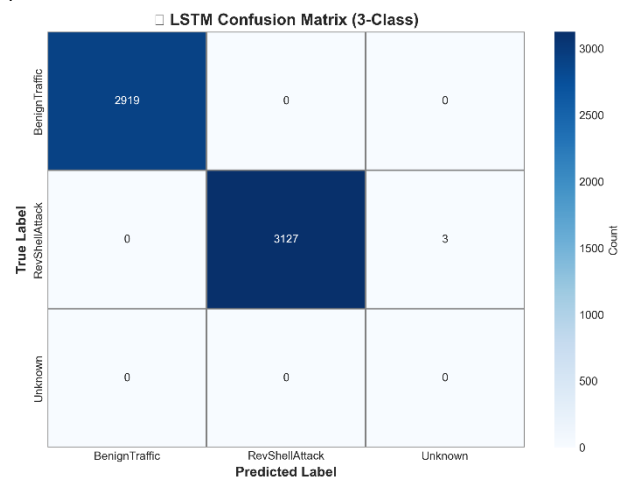


Fig. 4. Confusion matrix results in LSTM architecture.

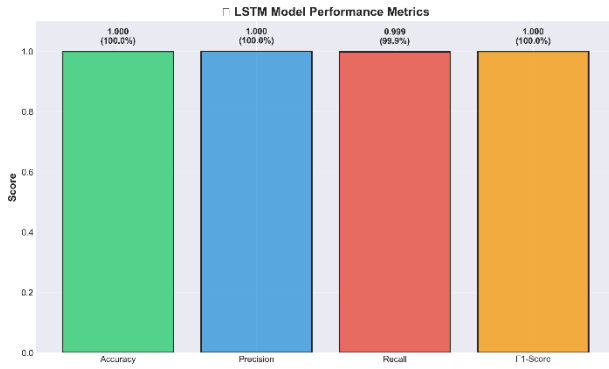


Fig. 5. Accuracy, precision, recall and F1-score of a LSTM

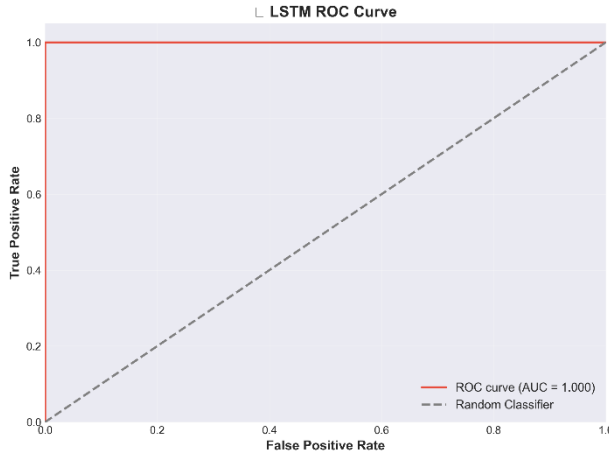


Fig. 6. LSTM performance evaluation via Receiver Operating Characteristics.

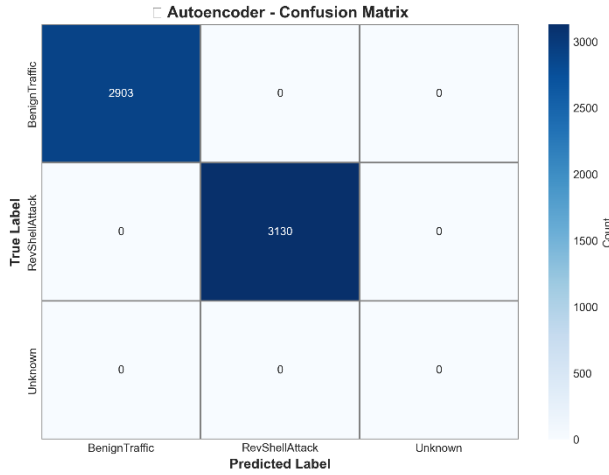


Fig. 7. Confusion matrix results in Autoencoder architecture

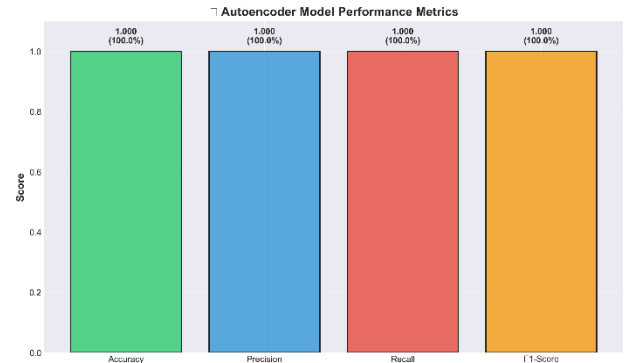


Fig. 8. Accuracy, precision, recall and F1-score of an Autoencoder

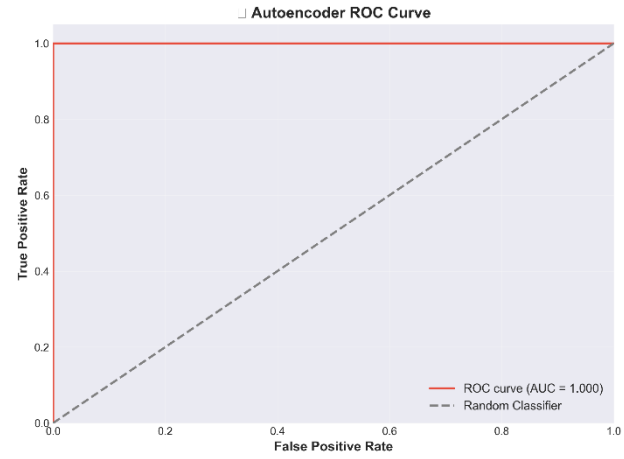


Fig. 9. Autoencoder performance evaluation via Receiver Operating

Table 2 compares the three neural architectures considered in this study with the 8 models considered in section 2 - Overview of existing solutions.

TABLE 2 COMPARISON OF OF DEEP NEURAL MODELS

Study	Year	Model	Dataset	Accuracy	Attack type
Present study	2026	LSTM	real live traffic	99.95%	Reverse Shell Attack + Unknown

Present study	2026	1D CNN	real live traffic	99.92%	Reverse Shell Attack + Unknown
Present study	2026	Autoencoder	real live traffic	100%	Reverse Shell Attack + Unknown
[1]	2025	Attention-CNN-LSTM	Bot-IoT	97.5%	Multi-class
[1]	2025	Attention-CNN-LSTM	NSL-KDD	94.8%	Multi-class
[2]	2025	CNN-Autoencoder	GPVS-Faults	98.84%	photovoltaic data
[3]	2025	Hybrid Autoencoder/HAE и Hybrid Residual LSTM-CNN	NSL-KDD, UNSW-NB1, CICIDS-2018	~98-99%	Multi-class
[4]	2024	CNN + Bidirectional LSTM	NSL-KDD	99.78%,	Multi-class
[4]	2024	CNN + Bidirectional LSTM	UNSW-NB15	98.96%	Multi-class
[5]	2024	CNN-LSTM	InSDN	98.20% - 99.01%	SDN-attacks
[5]	2024	Transformer	InSDN	98.50% - 99.02%	SDN-attacks
[6]	2022	Autoencoder-LSTM/BiLSTM	NSL-KDD	89%	Multi-class
[7]	2022	CNN based models	KDD Cup99	~98%-99.9%	Multi-class
[7]	2022	CNN based models	NSL-KDD	~95%-99%	Multi-class
[7]	2022	CNN based models	UNSW-NB15	~ 80% - 90% (CNN), 90% - 99% (hybrid CNN)	Multi-class
[7]	2022	CNN based models	CIC-IDS2017	~98%-99.9%	Multi-class
[7]	2022	CNN based models	CSE-CIC-DS2018	~ 98%-99.9%	Multi-class
[8]	2025	NSL-KDD, CICIDS2017, BoT-IoT	LSTM based models	best score – 99%	Multi-class

The results obtained show that the proposed models (1D CNN, LSTM and autoencoder) achieve very high attack detection accuracy, reaching 100%. Compared to existing studies [1]–[8], where the accuracy usually varies between 95% and 99%, the proposed approaches demonstrate comparable or higher efficiency. It is important to note that the models proposed in the paper are tested on real network traffic, which makes them more applicable in practical conditions. In addition, an ability to detect unknown attacks is observed, which is a significant advantage over traditional methods trained on predefined classes.

V. CONCLUSIONS

The experimental results show very high detection accuracy, reaching 99.95% for the LSTM model, 99.92% for the 1D CNN, and 100% for the autoencoder. Compared to existing studies [1] – [8], where the accuracy typically varies between 95% and 99% on standard datasets such as NSL-KDD, CIC-IDS2017, and UNSW-NB15, the proposed models demonstrate better performance.

A significant advantage of the present study is the use of real network traffic.

Despite the results achieved, it should be noted that the very high accuracy, especially for the autoencoder, needs to be confirmed by simulating at least one more type of cyberattack. Furthermore, direct comparison with other studies is limited due to differences in the datasets and methodologies used.

Future work will be aimed at testing the models on more types of network attacks, improving their generalization ability, as well as their integration into systems for real-time network traffic analysis.

In conclusion, the obtained results confirm that deep learning represents an effective approach for detecting network attacks and has significant potential for improving modern cybersecurity systems.

ACKNOWLEDGEMENTS

This paper is created in favor of Bulgarian National Scientific program “Security and Defense”, Ministry Council decision No 731/21.10.2021, Agreement No Д01-

74/19.05.2022, Ministry Council decision No 386/07.05.2026.

REFERENCES

- [1] A. M. Alashjaee, "Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection," *Scientific Reports*, vol. 15, Art. no. 21856, 2025, <https://doi.org/10.1038/s41598-025-07706-y>.
- [2] S. Titouni et al., "Hybrid CNN-Autoencoder model for accurate and efficient fault diagnosis in grid-connected photovoltaic systems," *International Journal of Electrical Power & Energy Systems*, vol. 173, Art. no. 111454, Dec. 2025, <https://doi.org/10.1016/j.ijepes.2025.111454>.
- [3] Y. Xue, C. Kang, and H. Yu, "HAE-HRL: A network intrusion detection system utilizing a novel autoencoder and a hybrid enhanced LSTM-CNN-based residual network," *Computers & Security*, Art. no. 104328, 2025, <https://doi.org/10.1016/j.cose.2025.104328>.
- [4] M. Udurume, V. Shakhov, and I. Koo, "Comparative Analysis of Deep Convolutional Neural Network—Bidirectional Long Short-Term Memory and Machine Learning Methods in Intrusion Detection Systems," *Applied Sciences*, vol. 14, no. 16, Art. no. 6967, 2024, <https://doi.org/10.3390/app14166967>.
- [5] M. S. Ataa, E. E. Sanad, and R. A. El-khoribi, "Intrusion detection in software defined network using deep learning approaches," *Scientific Reports*, vol. 14, Art. no. 29159, 2024, <https://doi.org/10.1038/s41598-024-79001-1>.
- [6] E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, "A two-stage intrusion detection system with auto-encoder and LSTMs," *Applied Soft Computing*, vol. 128, Art. no. 108768, 2022, <https://doi.org/10.1016/j.asoc.2022.108768>.
- [7] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Applied Sciences*, vol. 12, Art. no. 8162, 2022, <https://doi.org/10.3390/app12168162>.
- [8] N. Dash, S. Chakravarty, A. K. Rath et al., "An optimized LSTM-based deep learning model for anomaly network intrusion detection," *Scientific Reports*, vol. 15, Art. no. 1554, 2025, <https://doi.org/10.1038/s41598-025-85248-z>.
- [9] L. G. Nikolov, "Email social engineering in action," in *Proceedings of International Scientific Conference “Defense Technologies” (DefTech 2024)*, Faculty of Artillery, Air Defense and Communication and Information Systems, 2024, ISSN 2815-4282, pp. 395–402.
- [10] L. G. Nikolov, "Social engineering cyberattacks," in *Proceedings of International Scientific Conference “Defense Technologies” (DefTech 2024)*, Faculty of Artillery, Air Defense and Communication and Information Systems, 2024, ISSN 2815-4282, pp. 403–408.

Improving Text Search Memory Efficiency with NSW Text Indexing

Dmytro Dashenkov

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
<https://orcid.org/0000-0001-9797-1863>

Serhii Smelyakov

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
<https://orcid.org/0000-0002-5791-2479>

Anastasiya Chupryna

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
<https://orcid.org/0000-0003-0394-9900>

Loreta Savulioniene

Faculty of Economics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
l.savulioniene@viko.lt

Dainius Savulionis

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
d.savulionis@eif.viko.lt

Paulius Sakalys

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
p.sakalys@eif.viko.lt

Abstract— Modern day full text search relies on a simple yet robust inverted index data structure to find documents matching a text query. However, this approach is limited by the required spelling checker, which often has memory requirements comparable to the index itself. In this work, a novel approach to text indexing is introduced. Based on the navigable small world data structure, it offers a two-in-one solution for search with built-in spelling correction, sacrificing some performance for a substantial memory economy. The proposed index, just like the conventional inverted index, uses separate tokens extracted from a document as the main building blocks. The tokens are organized in a graph, each node representing one token. The nodes list all the document identifiers for the documents where the token is found. The edges of the graph connect tokens that are similar in terms of edit distance. The proposed approach utilizes an arbitrary ranking function to find relevant documents, the state-of-the-art BM25 ranking function is recommended as a reasonable default. The function values are weighed to take the edit distance into account. The ability to process misspelled words allows avoiding maintaining a separate structure for spelling correction while still generating search results which account for possible misspellings in the query phrase. The search time losses are attributed to the neighbor exploration while traversing the navigable small world data structure, and thus can be mitigated by configuring the data structure to maintain a fairly low number of connections. Such a configuration also provides a hard limit to the number of edits allowed in a single query term. The paper discusses in detail the ways of picking the optimal parameters for the

algorithm, as well as the limitations of the proposed approach.

Keywords— full text search, memory efficiency, navigable small world, spelling correction.

I. INTRODUCTION

A. Motivation

Full text search is a computer science task of finding relevant documents in a large text corpus based on an arbitrary subset of words. With the modern developments in machine learning which allow high accuracy semantic search, based on embedding vector closeness, rather than word matching, full text search can still be used to increase search accuracy using a hybrid approach, where both semantic and full text results are gathered and ranked as a part of one set of search hits. In this paper, full text search is considered as a separate procedure, detached of the possible hybrid approaches.

Usually, text search includes these high-level steps:

1. Query spell checking and correction.
2. Stop word exclusion.
3. Query tokenization (stemming).
4. Inverted index lookup.
5. Hit ranking with a function, such as BM25.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.215>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

The described algorithm can be adjusted based on the needs of a specific system, for instance, a filter matching can be added typically after the inverted index lookup to skip certain documents based on a business logic rule.

The inverted index is a simple yet powerful data structure, which consists of a hashmap of tokens to sets of documents, most often, represented by document IDs, which contain the associated token. The structure allows maintaining large text corpus indexes with constant lookup time and constant in the best case and linear in the worst case insert time. Additional optimizations such as bloom filters and roaring bitmaps can be used to further speed up the lookup time.

However, the inverted index can only work for well-prepared text data on both the corpus and query sides. When dealing with user-generated data, spell checking is a key step of ensuring that full text search will yield expected results, effectively enabling any full text search setup to be fuzzy. Modern approaches to spell checking, such as the symmetric delete spelling correction algorithm, can achieve great performance yet leave a sizable memory footprint due to specialized data structures, which they build to operate efficiently.

During the past months, at the time of writing this paper, rapid access memory hardware is going through a phase of severe price increases. In this light, it becomes paramount to develop and implement into real-world production systems, approaches to various computer science problems, including full text search, which would reduce the need for memory intensive computations. In this paper, we introduce an approach to full-text search, that would severely decrease memory consumption for a price of a small lookup speed loss.

B. Related Works

Some of the remarkable works in the field of full text search improvements include the work [1], which uses pre-processing techniques on inverted indexes in order to make the full text search robust to typos, achieving quite low latency figures for the search procedure.

Another work [2] introduces the concept of interactive fuzzy search, which utilizes prefix-based lookup with error-correction, allowing the system to execute search while the user is typing.

Another approach to the task is evaluated in [3], which tests spelling correction approaches as a part of the ranking phase of the search, rather than the retrieval phase. This paper suggests that a standalone spelling correction preceding the search operation could, in some cases, hurt the retrieval accuracy.

Despite this, [4] supports the notion of spelling correction being paramount to the search process, indicating that most improvements to modern full text search lie in the usage of an appropriate spelling correction mechanism.

An alternative approach to index memory efficiency is introduced in [5], leveraging complex compression mechanisms in order to reduce the inverted index memory

footprint. As the approach proposed in this article does not get rid of the inverted index entirely, the methods described in [5] could prove useful for practitioners implementing the approach.

Works [6] and [7] illustrate the versatility of vector-based text indexing, highlighting the effectiveness of interoperability of semantic and text-based approach to processing large corpora.

Finally, recent developments in intellectual data analysis, laid out in [8], suggest that processing large amounts of data in a relational fashion, which, could also be presented in graph form, proves useful for storing and indexing purposes.

II. MATERIALS AND METHODS

A. Proposed solution

The proposed approach uses a navigable small world (NSW) data structure to index text data. NSW is an undirected graph which stores data items in nodes. The edges connect nodes which are closest to one another by definition of a selected closeness function. In the case of full text search, each node contains a word, or, more precisely, a token and the links the documents where the token occurs. The edges connect tokens which are closest to one another by edit distance.

Typically, in a NSW graph, there is an absolute limit count of edges one node may have. However, in the proposed approach, this parameter is replaced by the more meaningful max edit distance parameter, which limits how many edits could be done to token for the edge connection to still be required. The recommendation on selecting this parameter are provided in the Experiment section of this paper. Other parameters that are typically attributed to the NSW data structure are not relevant in this case.

Since each edge of the graph represents one or more edit operations, the edges are weighted with the edit count. This is an important property which allows using a ranking function which accounts for spelling correction. If such a function is not needed, the edge weights could be dropped.

It's worth noting that the graph could, depending on the text corpus and the chosen max edit distance, turn out to be disconnected. This is, however, not significant for practical purposes, since all the lookup operations will be limited to local exploration, as described below.

In order to access each specific token in the graph, a hashmap of string tokens to nodes is maintained.

The algorithm for building the NSW graph involves precalculating the edits that could be possibly made to each given token. The steps of the algorithm are as follows.

1. A new document is introduced. Tokenize the document with possible stemming in order to receive a set of district normalized tokens.
2. For each token, check if it is already present in the graph by querying the hashmap. If it is, add the reference to the new document (in practice, the document is referenced by a unique ID) to the node and continue to the next token.

3. If the token is not yet present in the graph, create a new node for the token and add a reference to the document.
4. Iterate over all the possible variants of the token, obtained by making the edit operations to the token's string value until the selected max edit distance is reached. Check if each of the variants is present in the graph. For the found nodes, create an edge between the found node and the new node.
5. Prune the repetitive edges by traversing the graph starting with the new node and deleting edges with a higher weight. This way, only one optimal path between two nodes is maintained at any time.

The need to create edges which represent two or more edit operations stems from the fact that some tokens do not have a valid path between them with only one edit hops. Consider words "cat" and "rat", which can be connected with a single edge with the weight of one, the words "cat" and "rate", which are connected with two hops, "cat" to "rat", and "rat" to "rate", and the words "cat" and "came", which can only be connected with a single edge with the weight of two, since neither "cate" nor "cam" are words that occur in a given corpus.

Due to the need to explore all the possible variants of the token within the edit distance, the time complexity of the insertion of a document is calculated as the average token size to the power of max edit distance and then multiplied by the document size, as shown in formula (1).

$$T_1 = O(m n^d), \quad (1)$$

where T_1 is the time complexity, m is the size of the document, n is the average size of the token, and d is the chosen max edit distance.

On practice, iterating over all possible edits is very time and memory consuming task. In order to optimize it, the corpus is first fed symmetric delete spelling correction algorithm, also known as SymSpell, which builds a special data structure for the edits. Then, while filling the graph, the SymSpell structure is used to locate all the known valid edits, significantly reducing the time needed for the index construction. After the index is built, the SymSpell structure is removed from memory.

Another practical time and memory optimization lies in scaling the effective edit distance for each token individually, depending on the token length. This means that the max edit distance becomes an upper limit for the effective edit distance, and 1 is taken as the lower limit, and the effective edit distance is computed using formula 2:

$$d' = \min(d, \max(1, s / 3)), \quad (2)$$

where d' is the effective edit distance, d is the configured max edit distance, s is the length of the token.

The search algorithm, however, utilizes the prebuilt NSW graph to jointly execute both the lookup and the spell

checking, bringing in better results for accidentally misspelled words. It's worth noting that the algorithm does not handle words that are misspelled to the point of not being valid tokens, but rather handles the case when the intended word is spelled as a similar yet different word. The Discussions portion of this paper contains an in-depth explanation of why this approach is useful. The search algorithm consists of the following steps.

1. Stop word exclusion.
2. Query tokenization (stemming).
3. For each of the tokens, the corresponding NSW graph node is looked up using the hashmap.
4. All the documents referenced in the node are added to the results to be ranked.
5. All the edges connecting to this node are explored. The graph is traversed in order of edit distance from the original node, from smallest to highest. All the found documents are added to the result for ranking with their edit distances memoized.
6. Once all the nodes are explored, the documents are ranked, and the rank values are weighed to include the information about the edit distance.

The lookup operation has the worst-case scenario time complexity of average query token size to the power of max edit distance then multiplied by the query size, as shown in formula (3).

$$T_2 = O(q n^d), \quad (3)$$

where T_2 is the time complexity, q is the size of the query, n is the average size of the token, and d is the chosen max edit distance.

In the best-case scenario, however, the node would not be connected to any other nodes and thus the time complexity would be linear, depending on the query size only. This best-case scenario, however, means that the NSW data structure did not bring any value to the search, since no misspelled variants were considered.

When ranking the collected hits, a BM25 function should suite most cases due to its versatility and high variability [9]. The computed rank scores for each token are multiplied by the inverse edit distance from the query token to the token from which each hit is resolved, as shown in formula (4).

$$f = \sum_{i=0}^N (BM25(t_i) / (d_i + 1)), \quad (4)$$

where f is the rank score of the hit, N is the number of query tokens, $BM25(t_i)$ is the rank score of the hit with regards to a specific token, d_i is the edit distance between the original query token and the token found in the document.

B. Experiment design

In order to check the suggested approach experimentally, a comparison is drawn between two search indexes.

Index A is built using the conventional method. Firstly, the corpus is split into separate words and stemming each word. An inverted index is built, maintaining a mapping between the resulting tokens of the corpus and the documents that contain those tokens. Next, a spelling correction data structure is built for the symmetric delete spelling correction algorithm. In this and all other occurrences, in order to make sure the spelling code is robust and as close as possible to a real-world scenario, the SymSpell component of the LanguageTool library [10] is used to build such a data structure and generate spelling corrections. A search operation on index A would involve tokenizing the query, looking up possible alternative spellings for each query token, gathering relevant documents via the inverted index, and finally ranking the documents.

Index B is built using the approach suggested in this paper. Firstly, just like in the index A process, the corpus is tokenized by splitting the texts into words and stemming each word. Next, an NSW graph is built with the tokens, as described above. In order to speed up the graph building process, a temporary SymSpell instance is created with all the tokens of the corpus. This is a shorthand way of generating valid alternative spellings for each token, once the NSW graph is built, the SymSpell instance is deleted, freeing up memory.

The corpus chosen for the test is the corpus of Simple English Wikipedia articles. A 10K article subset is used, containing 42 unique tokens and 42 total, averaging 42 tokens per article. Each article consists just of the title and a plain text content, both indexed equally for this experiment.

III. RESULTS AND DISCUSSION

A. Experimental findings

The proposed approach has one important parameter, the edit distance between the tokens. In order to compare the memory usages of the conventional and the proposed approaches, a series of experiments with different values of max edit distance was conducted. The results of the described experiments are provided in the table 1.

TABLE 1 INDEX MEMORY FOOTPRINT

Max edit distance	Memory Footprint, MB	
	Index A	Index B
0 (no spell checking)	22	25
1	22	45
2	22	52
3	108	62
4	110	65
5	118	66

As shown in the table, across all the edit distance limits, the NSW-based approach (index B) requires less memory

to store all the required indexes that the conventional approach (index A). The main reason for this is the fact that the SymSpell data structure requires more information to error-correct queries than the NSW graph, since the graph only stores valid misspellings, while the SymSpell stores all the possible edits of a token.

Next, the search speed was measured. Table 2 provides latency per 100 search operations with the same query phrases for all the configurations described above.

TABLE 2 SEARCH LATENCY

Max edit distance	Memory Footprint, MB	
	Index A	Index B
0 (no spell checking)	6	54
1	15	73
2	17	166
3	23	1318
4	59	2066
5	185	2476

The figures provided in table 2 are merely indicative of the amount of work required for each search configuration. The measurements were conducted in single-thread environment with no attempts of optimization, yet they allow understanding the scale of the trade-off when switching from a more conventional indexing approach to the suggested one. Time for scoring hits with a ranking function, such as BM25 is not included, as it is not variable between the index methods.

B. Discussions

In this paper, the edges of the graph represent edit operations. Edge weights are always integer and represent the edit distance between the two connected word nodes. However, in practice, there might be some value in distinguishing different text edits and assigning different weights to them, based on, for instance, probability of a typo that would cause that edit. In this scenario, a missing letter would have one probability, an extra letter may have another probability, and the letter swaps would each have their own probabilities, based on how often do people mistype one word or another. This might provide additional potency to the spell-checking aspect of the algorithm, allowing different typos to influence the final ranking score more or less depending on their likelihood. Further research is needed to compile a dataset of typo probabilities and test this approach.

This paper describes spell checking a search algorithm with integrated spell checking. However, the spell-checking aspect is limited to switching between valid tokens and does not cover the case of completely misspelled words. In the modern practical applications, this is often enough, since queries might go through a client-side spell checker, which would eliminate any misspelled words but retain words that are present in the spell

checker's dictionary, allowing typos like "cat" – "rat" to happen.

If the assumption of a client-side spell checker cannot be made, a simple modification is suggested to the graph building algorithm, which allow the index to support any kind of misspellings. For this, is an edited variant of the token is not found in the graph, it must be created and linked to the original token. No documents are linked to that extra node, signifying that it does not represent a valid token, but is merely a synthetic node. Now, if a misspelled query token is passed to the search, the graph traversal will begin with this synthetic token and the search will proceed from it to the tokens with linked documents. Given this modification to the data structure, if a query token is present in the index, it is guaranteed that some result hits will be passed to ranking. The opposite is true as well, when a token is not found in the index, no hits will be produced for that token. This is a good baseline for most systems, though, it comes at a cost of using extra memory for storing the synthetic nodes.

All things considered, the suggested approach offers an adequate alternative to modern methods of indexing text data. Another benefit of constructing an NSW graph is the interoperability with the hierarchical navigable small world (HNSW) graph indexes built for semantic search. Since the two data structures have similar properties (HNSW being a more advanced version of NSW), it is easy to consider a hybrid approach, where one graph hosts both document vectors and separate tokens, allowing to search via both modes in a single traversal operation. In this case, hierarchical nature of the HNSW graph would provide an obvious entry point to the traversal, potentially eliminating the need for both nodes with no linked documents and a hashmap pointing to all each of the nodes. Given the rise of popularity of hybrid approaches to search, the coexistence of the two indexes in one structure could prove useful in many practical applications. The details of such coexistence must be further researched, however, similar approaches are suggested by researchers behind the Allan-Poe graph index, which combines text, vector, and knowledge graph information all in one data structure [11].

IV. CONCLUSIONS

In this paper, a novel approach to indexing text data is proposed, which spelling correction with search. The approach shows a more efficient memory usage for the static data structures (indexes) when compared to a more conventional correct-then-search approach. Also, by connecting tokens that are close by edit distance to one another, the user of the index gains the ability to correct typos, allowing for a more precise search, when a query token which contains a typo is accompanied by one of a few tokens which do not. Thus, the approach provides both memory savings and formalizes fuzzy ranking formula using BM25 weighed with respect to the edit distance between the query token and the hit token.

The suggested approach compromises on search speed when compared to non-spell-checking search, but matches the search of a spell-checking approach with similar spell-checking mechanisms.

The promising notion of combining the NSW approach with a vector-based semantic search would further improve state-of-the-art hybrid search systems, consolidating the two search modes into one graph traversal operation, which, in order, simplifies ranking. Such approach is already explored by other researchers and could yet still be improved with an edit-distance-based edge building strategy.

REFERENCES

- [1] H. Bast and M. Celikik, "Efficient fuzzy search in large text collections," *ACM Transactions on Information Systems*, vol. 31, no. 2, pp. 1–59, May 2013, doi: <https://doi.org/10.1145/2457465.2457470>.
- [2] S. Ji, G. Li, C. Li, and J. Feng, "Efficient interactive fuzzy keyword search," *The Web Conference*, Apr. 2009, doi: <https://doi.org/10.1145/1526709.1526760>.
- [3] I. Zelch, G. Lahmann, and M. Hagen, "Embedding-based Query Spelling Correction," in *WOWS'24: 1st International Workshop on Open Web Search*, Glasgow, Scotland, Mar. 2024. Accessed: Apr. 08, 2026. [Online]. Available: https://ceur-ws.org/Vol-3689/WOWS_2024_paper_4.pdf
- [4] S. K. Singh, "Spelling Correction in Healthcare Query-Answer Systems: Methods, Retrieval Impact, and Empirical Evaluation," *arXiv.org*, Feb. 2026, doi: <https://doi.org/10.48550/arXiv.2603.19249>.
- [5] C. Kamphuis, P. de Vries, L. Boytsov, and J. Lin, "Which BM25 Do You Mean? A Large-Scale Reproducibility Study of Scoring Variants," in *Advances in Information Retrieval*, Springer Science+Business Media, Apr. 2020, pp. 28–34. doi: https://doi.org/10.1007/978-3-030-45442-5_4.
- [6] R. Lynnyk, V. Vysotska, Z. Hu, D. Uhryn, L. Diachenko, and K. Smelyakov, "Information Technology for Modelling Social Trends in Telegram Using E5 Vectors and Hybrid Cluster Analysis," *International Journal of Information Technology and Computer Science*, vol. 17, no. 4, pp. 80–119, Aug. 2025, doi: <https://doi.org/10.5815/ijitcs.2025.04.07>.
- [7] V. Vysotska, K. Smelyakov, A. Chupryna, M. Derenskyi, V. Repikhov, and M. Hvozdiyev, "AI assistant for intelligent interaction and route optimization in offshore turbine maintenance system," *Proceedings of the PhD Workshop on Artificial Intelligence in Computer Science at 9th International Conference on Computational Linguistics and Intelligent Systems (CoLInS-2025)*, vol. 4015, May 2025, doi: <https://doi.org/10.31110/colins/2025-3/001>.
- [8] V. Filatov, O. Zolotukhin, and M. Kudryavtseva, "Intellectual data analysis in relational information and analytical systems," *Innovative Technologies And Scientific Solutions For Industries*, no. 4(34), pp. 101–111, Dec. 2025, doi: <https://doi.org/10.30837/2522-9818.2025.4.101>.
- [9] G. E. Pibiri and R. Venturini, "Techniques for Inverted Index Compression," *ACM Computing Surveys*, vol. 53, no. 6, pp. 1–36, Feb. 2021, doi: <https://doi.org/10.1145/3415148>.
- [10] "languagetool-org/languagetool," 2024, gitHub repository. [Online]. Available: <https://github.com/languagetool-org/languagetool>
- [11] Z. Li, Y. Li, Y. Zhu, C. Ge, Z. Chen, and Y. Gao, "All-in-one Graph-based Indexing for Hybrid Search on GPUs," *arXiv.org*, 2025, doi: <https://doi.org/10.48550/arXiv.2511.00855>.

Determining the Organizational Level of Digital Maturity from the Integration of AI in the Service Sector in the Republic of Bulgaria

Gergana Sl. Dimcheva

Management in communications Department,
University of Telecommunications and Post,
Sofia, Bulgaria
g.dimcheva@utp.bg

Ivaylo Ts. Stoyanov

Management in communications Department,
University of Telecommunications and Post,
Sofia, Bulgaria
i.ts.stoyanov@utp.bg

Abstract — In recent years, in the context of digital transformation, the concept of "digital maturity" has been increasingly used. The purpose of this study is to determine the organizational level of digital maturity of organizations in the service sector in the Republic of Bulgaria, in the context of the integration of technologies based on artificial intelligence. The focus is on identifying the main aspects that facilitate or hinder the process of their successful integration and effective application. In connection with the set goal, an empirical study was conducted among managers and IT experts from selected companies in the sector, on the territory of the Republic of Bulgaria.

Keywords— Artificial intelligence, digital maturity, digital transformation, services.

I. INTRODUCTION

With the development of the fourth and transition to the fifth industrial revolutions, the digital transformation of business has become a fundamental foundation for adapting companies to new technologies that will dominate a high-tech and platform-oriented business model. In this sense, digital transformation has become a new stage of industrial development where the competitiveness of business structures is determined by the creation, integration and adaptation of digital technologies and their application in relationships with customers and stakeholders. This requires not only a technological, strategic and cultural rethinking of business, but also a new approach to the activities and processes for creating products and services to improve the customer experience and reduce costs. In the context of technology-oriented business, digital transformation requires companies to create value by effectively managing changes in the digital environment, adapting to customer requirements and implementing new achievements in the field of high technologies.

As digital transformation changes the concept of the business model of organizations, in addition to having to implement new technological solutions for business process optimization, they redirect their strategic efforts, competencies, resources and technological capabilities into digital business practices. This requires a fundamental change in organizational culture and a new approach to managing corporate business in a technologically oriented competitive environment. In this aspect, digital maturity is perceived as the tool through which organizations can gain insight into real business in a digital environment, to assess their capabilities and abilities to integrate modern technologies (including AI) into the applied digital business model. That is, digital maturity turns out to be a key mechanism for technology-oriented companies to diagnose their digital business practices, to assess their suitability for the digital environment, the level of technology application, the allocation of resources and the impact on customers and stakeholders. Digital maturity is a comprehensive approach to determining the organizational level for the effective use of high technologies and corporate competitiveness in individual aspects of business.

Digital maturity is a necessary tool in the context of digital business transformation, because it helps organizations gain a clear understanding of the integration of technological trends and assessment of digital practices in the context of digital sustainability and competitiveness. It should be applied at a certain time interval in the technological development of organizations, to track the management of business processes and key performance indicators of business models. The main goal of companies is to establish a high level of digital maturity from digital business transformation initiatives, so as to establish their advantages in a digital environment. On the other hand, digital maturity helps companies identify weaknesses in achieving goals and where the problems are in the field of

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.92>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

technological leadership, implementation of the digital strategy, transition or a new stage of development of digital culture, digital customer service, competitiveness, etc. Based on the data obtained from the approach to determining the level of digital maturity of companies, methods and techniques for increasing the strategic and operational efficiency of the implementation of the business model are highlighted. This helps develop a structured plan to optimize digital transformation processes, use cutting-edge technology solutions, better customer experience from the purchase of technology-based products and services, and sustainable growth.

In the scientific literature and digital practice of organizations, there are different areas for determining the level of digital maturity in the process of digital transformation [1], [2]. These areas are precursors of the applied models, which form a structured framework that organizations can skilfully use to diagnose and assess digital opportunities and gaps in the business and, accordingly, determine the level (position) of their digital maturity. Six main areas for determining the level of digital maturity of organizations stand out - strategy and organizational culture, technology, customers, innovation, human factor and operations [3], [4], [5]. From the point of view of strategy and organizational culture, digital maturity generally measures the degree of readiness of organizations for management in a digital environment. The assessment of the digital strategy shows how organizations use digital technologies to achieve business goals and priorities. As for the assessment of the digital organizational culture, it determines to what extent hierarchical relationships and frequent control have been removed, how communication is carried out between employees, customers and stakeholders, what is the digital leadership potential, people's engagement with the digital transformation, behaviour and practices of work in a digital environment. In a technological aspect, digital maturity encompasses key indicators for determining the level of digital IT infrastructure, the use of cutting-edge technological tools (e.g. AI), business process automation, determining the degree of efficiency of the technological architecture for information processing, use of information system resources, etc. [6], [7], [8].

The goal of organizations in this area of digital transformation is to assess the extent to which digital technologies are implemented and effectively used in digital business. Customers are a priority area of every digital business because they determine the demand for products and services in technological platforms and the online environment. Digital maturity in this aspect of business aims to determine the extent to which organizations emphasize the external online focus on customers to add value, promote and evaluate the brand, opportunities to improve satisfaction and customer experience from the purchase, the company's personal attitude to customer needs and feedback on the results. Today, business is accessible to every point on the planet because customers have the technological capabilities and means (computers, laptops, smart phones, tablets) to search and choose products and services that satisfy them in

indicators such as price, quality, delivery time, costs and user value.

The goal of organizations in this area of digital maturity is to assess the extent to which digital technologies and tools are used to improve customer interaction, engage their attention and choose the preferred digital channels for access and business relationships. Innovation in a technological environment is an important component of corporate competitiveness because it allows for the integration of new technologies and technological solutions into the business. Digital maturity helps organizations determine the level of effectiveness of innovative digital platforms, business models, innovative ecosystems and opportunities to implement innovative business practices. Determining the organizational level of digital maturity from the human factor perspective aims to assess the extent to which people have the necessary digital competencies, how they adapt to the digital organizational culture, how to search for and retain talent and what is the effectiveness of the human factor in a digital business environment. From an operations perspective, digital maturity measures the level at which digital business activities and processes are designed, redesigned, implemented and managed so as to increase efficiency and make the business competitive.

In the scientific literature and digital practice of organizations, various digital maturity models are applied that help determine the level of effectiveness in a selected segment (priority area) of digital business [9], [10]. They help organizations regularly track progress in implementing digital transformation and, of course, can explore a specific area to determine the level of digital maturity. This approach is important for digital business because it assesses the abilities of organizations to integrate digital practices and tools into modern business, to create technology-based innovations and business processes. Determining the organizational level of digital maturity helps companies implement the digital transformation plan, regularly track progress or lagging behind competitors. Digital maturity is a certificate for companies to respond adequately and methodically to new challenges in digital business, to determine what the next steps should be to integrate cutting-edge technologies into the business, achieve business goals, customer satisfaction, competitiveness and return on investment.

Obviously, digital maturity models help companies determine their current state in the digital transformation cycle and take the necessary steps to achieve goals in the field of digital technologies and systems. Several well-known models for assessing digital maturity are applied in the digital practice of organizations (for example, Deloitte DMM, BCG's Digital Acceleration Index, TM Forum Model, Digitopia DAIMI, Digital Maturity Assessment Model DMAM, Capability Maturity Model Integration CMMI, etc.) [11], [12], [13]. Their application in the field of digital business transformation can be a good catalyst for assessing and future planning of digital initiatives, resources and strategies for sustainable growth. These models provide a structured framework for assessing digital effectiveness, regardless of the industry sector in

which companies are developing or their size. When it comes to the practical application of a specific model in a given organization, it is necessary to determine what effect it will have on the assessment of digital business, how it will provide the necessary information and guidelines for action to increase efficiency. In this regard, it is recommended to consider several important criteria [14], [15], [16]. The selected model should be focused on the general context of the digital business or a selected segment (area) of it, it is good to take into account the specifics of the industry and the service sector, to report progress over a long period of time, to provide relevant data for comparison with competitors or adopted standards and to have practical application in different levels of digital maturity. From the point of view of comparing the results (indicators) in the different indicators of digital maturity of organizations, it is important to conduct a comparative analysis against those of competitors. This strategic approach will allow companies to optimize their digital strategies and business practices, based on good digital practices in the industry or branch in which they operate. In this way, they can accelerate the process of digital maturity, taking into account the specifics of the business and the planned key performance indicators. Typically, the results are associated with a better understanding of the current state of the companies' digital business, what are the priorities of digital initiatives and the necessary resources for working in a digital environment. The strategic innovations that are the basis of the technological development of companies and digital trends in the business sphere should not be underestimated. The factors on which competitiveness depends, strategies for countering competitors and choosing digital niches for optimal business efficiency are also determined.

Considering the comparison of the results (indicators) in the different indicators of digital maturity of organizations, it is important to apply an appropriate approach [17], [18]. Usually in the practice of companies, a periodic assessment of digital maturity is made, which covers the main components of the digital business, the current capabilities of the organizations, the available resources and the desired results. Then, information is generated from leading companies in the industry or branch and an analysis of their good practices is made with an emphasis on the strong aspects of the business and the opportunities for improving KPIs.

It is especially important to make strategic analyses and recommendations for improving digital maturity in various aspects of the assessment of business components and to develop a roadmap for achieving the expected level of digital maturity. It is also necessary to follow the process of determining progress, which enables organizations to continuously improve and develop. Of course, the comparative analysis of digital maturity should focus on key (or problematic) components of the organization's business. Often, such activities and processes related to the priority areas of digital transformation are determined - technology and innovation, personalization, engagement and customer experience, work and behavior of the human factor, strategies and tactics for operational efficiency.

Digital maturity models have advantages in terms of assessing the real state of companies and predicting future actions in a digital environment [19], [20]. In addition, some limitations and considerations arise, the most important of which are related to the subjective assessments of analysts, their perception as a framework for mandatory implementation (it only directs implementers to decisions and actions that depend on the context of digital business practices) and the understanding that the relevant model will solve all the problems of organizations in digital transformation. It is good to make a choice of an appropriate model, according to the relevant stages and their importance for the digital business of companies or to approach globally with a scientific purpose (as in the practical part of the publication), by determining the organizational level of digital maturity in a specific area of companies in a specific industry sector. This is done through surveys, interviews, comparisons through data analysis, a comprehensive assessment of the digital business, etc.

Determining the organizational level of digital maturity goes through various steps that depend on the specifics of the company's business, the industry in which it operates and the goals when choosing an assessment model. These steps help organizations to establish the actually achieved results with the previously planned goals and performance indicators [21], [22], [23]. In the context of digital maturity, the steps have a specific application focus, with the main ones having the following specificity. First, a connection is sought between the set goals and the desired performance indicators, which must be clearly defined, measurable and achievable. Second, information is generated for a specific area (or areas) that will be the subject of assessment.

On the one hand, this helps companies understand the mechanism by which digital transformation works, and on the other hand, how individual systems, technologies and business processes interact in the value chain. Thirdly, a comparative analysis is made with adopted performance indicators or certain standards, so as to identify the activities and processes that are of strategic importance to companies and those that hinder their digital development. Fourthly, a detailed analysis of the results obtained is made, priorities for increasing digital efficiency are ranked and measures for redesigning inefficient activities and processes are identified. Fifthly, conditions are created for planning potential changes that will improve digital transformation and the resilience of companies to technology-oriented business practices and competitive digital strategies.

II. MATERIALS AND METHODS

The aim of this study is to determine the organizational level of digital maturity of organizations based on a survey of managers and IT experts from randomly selected companies in the service sector, in the context of the integration of artificial intelligence-based technologies. The focus is on identifying the main aspects that facilitate or hinder the process of their successful integration and effective application.

The study is preliminary (pilot), and its scope is quite sufficient to obtain a real idea of the degree of digital maturity in small and medium-sized enterprises in the service sector, as well as to outline the main trends, attitudes and challenges related to the implementation of technologies based on artificial intelligence. The study also allows to identify key factors determining the readiness of organizations for technological adaptation and development. The results obtained and the applied methodology will serve as the basis for a subsequent expanded study with a larger sample size, additional indicators and a more in-depth comparative analysis between organizations from different economic sectors of the economy.

The survey was conducted in four major cities in the Republic of Bulgaria – Sofia, Plovdiv, Burgas and Ruse. The survey was randomly sent to 31 organizations in the service sector. The completed and returned surveys were from a total of 76 respondents, representing 24 organizations. The sample mainly includes representatives of senior management (32%) (owners/managers setting strategic development goals) and middle management/head of departments (38%) (operational managers implementing digital tools), as well as IT experts (17%) (usually these are managers who have technical expertise in implementing a given infrastructure). In terms of the size of the surveyed companies, according to the criterion “Number of employees”, micro-enterprises with up to 10 employees (58%) and small and medium-sized enterprises with 11-50 employees (29%), and organizations with employees between 51-250 employees – 13%.

The research focuses on small and medium-sized enterprises (SMEs), as unlike large companies that have not only financial security but also expert capacity, SMEs in Bulgaria often face limited financial, technological, human resources, as well as barriers to the integration of artificial intelligence. A quantitative approach was adopted to conduct the study through an online survey for a period of three months (December 2025 to February 2026).

The survey questions are 15 in total and are structured in five areas for studying digital maturity, namely: Digital maturity at the level of strategic initiatives of senior management; Digital maturity at the level of organizational culture; Digital maturity at the level of human resources; Digital maturity at the level of technological infrastructure and Digital maturity at the level of automation and artificial intelligence. The questions are combined - questions on a 5-point Likert scale, closed questions with pre-set statements and several open-ended questions. The questionnaire was developed to assess both the current level of digital maturity and the readiness of organizations for the implementation and integration of technologies based on artificial intelligence in small and medium-sized enterprises in the service sector. Due to limitations in the volume of the publication, the full version of the questionnaire is not attached to this article, and only a part of the results obtained are presented.

The areas defined in the study are based on theoretical and applied models for determining digital maturity [3],

[4], [5], [9], [10], [24], [25], [26], which allow for a comprehensive assessment of the readiness of modern organizations for technological transformation.

III. RESULTS AND DISCUSSION

The following figures reveal the key factors that limit or stimulate the achievement of digital maturity in small and medium-sized enterprises in Bulgaria. The distribution of responses regarding the role of management in the process of digital transformation and implementation of artificial intelligence is presented in Fig. 1.

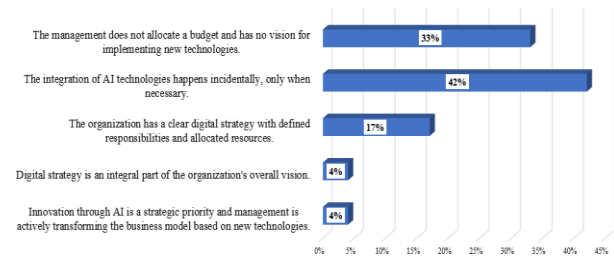


Fig. 1. Answer to the question "What is the role of management in the process of digital transformation and AI?"

The following figure (Fig. 2) illustrates the level of digital maturity at the organizational culture level, reflecting the attitudes of employees in the surveyed organizations towards new technologies and artificial intelligence.

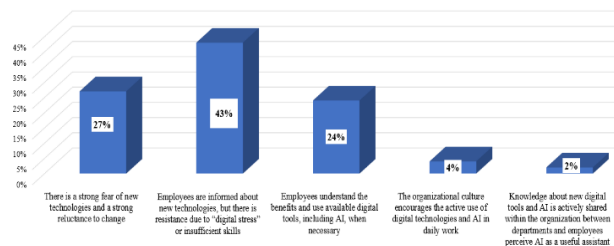


Fig. 2. Answer to the question "What is the attitude of employees in your organization and the organizational culture towards new digital technologies, including AI?"

The distribution of responses describing the level of digital competencies of human resources when working with artificial intelligence are presented in Table 1.

TABLE 1 LEVEL OF EMPLOYEE TRAINING FOR WORKING WITH ARTIFICIAL INTELLIGENCE-BASED TECHNOLOGIES

Level of competence and training	Relative share of respondents (%)
Employees do not have the necessary skills to work with AI-based technologies, and the organization does not invest in training.	50%
Employees have basic digital skills, but face difficulties when working with AI, and training is conducted only when absolutely necessary.	31%
A significant part of employees have the necessary skills to work with AI, as the organization conducts periodic training.	8%
Employees have the necessary skills to work with AI on a daily basis, as the organization regularly invests in specialized training.	7%

All employees are highly competent in working with AI, and the organization has its own experts for the implementation and development of AI-based tools.	4%
Total	100%

Fig. 3 presents the distribution of responses that most accurately describe the state of the IT infrastructure in the surveyed enterprises and their readiness for the integration of AI technologies.

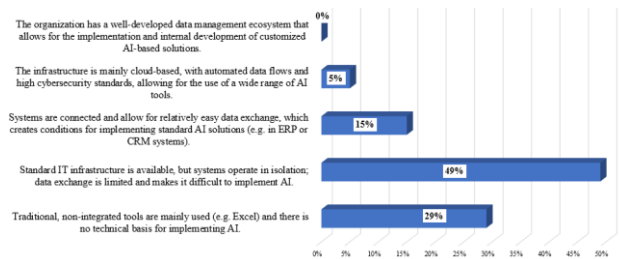


Fig. 3. Answer to the question "Which of the following statements best describes the state of your IT infrastructure and its readiness for implementing solutions based on artificial intelligence (AI)?"

The following Table 2 shows the digital maturity at the automation level, reflecting the degree of real application of artificial intelligence technologies in the business processes of the surveyed organizations.

TABLE 2 DEGREE OF REAL APPLICATION OF AI TECHNOLOGIES IN BUSINESS PROCESSES

Level of competence and training	Relative share of respondents (%)
We do not use AI tools and have no plans to implement them in the next two years.	42%
Incidental and unsystematic use of ready-made free tools (e.g. ChatGPT, Canva) by individual employees for administrative tasks.	29%
Targeted use of AI primarily for optimization of individual auxiliary processes and daily tasks.	13%
Targeted use of AI primarily for optimization of core processes, marketing, risk assessment or customer service.	12%
We use customized AI solutions, which are a leading factor in our operational efficiency and competitiveness.	4%
Total	100%

The gradual integration of modern technologies and the systematic development of human capital are critical factors for the transition to higher levels of digital maturity. Since the lack of specific expertise is a leading barrier to the implementation of artificial intelligence for 72.7% [27] of enterprises in Bulgaria, targeted training programs are crucial to overcome resistance to change and mitigate "digital stress". This allows SMEs to move from incidental experimentation and the use of AI only when necessary to the transformation of business processes through the systematic integration of AI tools.

The results in Fig. 1 show that according to 42% of respondents, the integration of AI in the organizations they belong to happens incidentally, and 33% of managers do

not have a vision and do not allocate a budget for the implementation of new technologies. Only 4% indicate that organizations consider AI as a strategic priority and according to 4% - the digital strategy is an integral part of the overall vision of the organization. In the second direction regarding digital maturity at the level of organizational culture (Fig. 2), the results show serious barriers related to resistance to new technologies due to "digital stress" and lack of sufficient skills (43%), while 27% of staff have a pronounced fear and strong reluctance to change. Only 4% of respondents indicate that they work in an environment that encourages active sharing of knowledge related to AI.

The trend of low digital maturity is also confirmed in the third area of research, related to human resources, which is confirmed by the results in Table 1. A total of 81% of those surveyed experience serious difficulties related to human capital, which makes the lack of competencies a major barrier to their technological adaptation. According to 50% of those surveyed, employees do not have the necessary skills to work with AI, but at the same time, organizations do not invest in training. Another 31% believe that employees have basic skills, and training is conducted only when absolutely necessary, despite the fact that they face difficulties when working with AI. On the other hand, the remaining 19% of those surveyed are aware of the need for human resources development. According to only 4%, the companies they belong to have highly specialized internal experts.

In addition to management and personnel challenges, the integration of AI in Bulgaria also faces a serious technological barrier, which is confirmed by the results in Figure 3. Nearly half of those surveyed (49%) report incompatibility of new technologies with existing systems that operate in isolation. A critical indicator of low digital maturity at the level of technological infrastructure is the fact that, according to 29% of respondents, organizations still use mainly traditional, non-integrated tools (e.g. Excel) and there is a complete lack of technical basis for implementing AI solutions.

Regarding the answer to the question of system connectivity, only 15% of respondents indicated that their systems allow for relatively easy data exchange, which creates conditions for the implementation of standard AI solutions within ERP or CRM systems. This result is in full harmony with the trends on a national scale. According to official NSI data for 2025, a total of 11.9% use CRM systems, and 26.6% - ERP systems (NSI, 2025). Based on these results, it can be concluded that technological infrastructure remains a key obstacle to the larger-scale penetration of artificial intelligence in small and medium-sized enterprises in the service sector.

The results for the fifth research area, namely "Digital maturity at the level of automation and AI", reveal the real state of technological transformation in the organizations studied. Table 2 shows that the largest group of enterprises do not use AI tools and do not have plans for implementation in the next two years, i.e. These are organizations that are characterized by low innovation and

lack of management vision. Nearly a third (29%) believe that companies use AI incidentally and unsystematically using ready-made free tools (e.g. ChatGPT, Canva) by individual employees for administrative tasks. A total of 25% indicate that organizations use AI purposefully – 13% mainly for optimization of individual auxiliary processes and daily tasks, and 12% - mainly for optimization of core processes, marketing, risk assessment or customer service.

CONCLUSIONS

The study shows that the integration of AI in small and medium-sized enterprises in the service sector in Bulgaria is still in the “exploration” or “incidental experimentation” stage, i.e. if it is to be defined as a level of digital maturity – “initial” or “developing” level of digital maturity. The transition to a systemic transformation of business processes based on AI solutions requires not only technological modernization, but also continuous improvement of human resources in order to overcome the barrier of lack of skills. All this requires direct commitment of senior management by setting a target budget for innovation, developing a clear digital strategy with defined responsibilities and provided resources, which is an integral part of the overall vision of the organization.

ACKNOWLEDGMENTS

This research was funded by supported in part by the Research and Development Activity at the University of Telecommunications and Post, Sofia, Bulgaria, Project Number 44/30.03.2026.

REFERENCES

- [1] H. Jie, L. Gooi and Y. Lou, "Digital maturity, dynamic capabilities and innovation performance in high-tech SMEs," *International Review of Economics & Finance*, Elsevier, Vol. 99, 2025, [Online]. Available: ScienceDirect, <https://www.sciencedirect.com>. [Accessed: Febr. 3, 2026], <https://doi.org/10.1016/j.iref.2025.103971>
- [2] G. Quenum, S. Vallée and M. Ertz, "The digital maturity of small- and medium-sized enterprises in the Saguenay-Lac-Saint-Jean region", vol. 13, no. 9, p. 835, 2025. [Online]. Available: MDPI, <https://www.mdpi.com>. [Accessed: Mar. 13, 2026], <https://doi.org/10.3390/machines13090835>
- [3] M. Borštnar and A. Pucihar, "Multi-attribute assessment of digital maturity of SMEs", *Electronics*, vol. 10, p. 885, 2021. [Online]. Available: MDPI, <https://www.mdpi.com>. [Accessed: Febr. 13, 2026], <https://doi.org/10.3390/electronics10080885>
- [4] A. Tubis, "Digital maturity assessment model for the organizational and process dimensions", 2023, *Sustainability*, vol. 15, no. 20, p. 15122, 2023. [Online]. Available: MDPI, <https://www.mdpi.com>. [Accessed: Febr. 8, 2026], <https://doi.org/10.3390/su152015122>
- [5] M. Mick, J. Kovaleski, R. Mick and D. Chiroli, "Developing a sustainable digital transformation roadmap for SMEs: Integrating digital maturity and strategic alignment," *Sustainability*, vol. 16, no. 20, 2024. [Online]. Available: Semantic Scholar, <https://www.semanticscholar.org>. [Accessed: Febr. 16, 2026], <https://api.semanticscholar.org/CorpusID:273278988>
- [6] G. Brătuțu, E. Ciobanu, I.B. Chițu, A.V. Litră, Zamfirache and M. Bălășescu, "The use of technology assisted by Artificial Intelligence depending on the companies: Digital maturity level", *Electronics*, vol. 13, no. 9, p. 1687, 2024. [Online]. Available: MDPI, <https://www.mdpi.com>. [Accessed: Mar. 12, 2026], <https://doi.org/10.3390/electronics13091687>
- [7] O. Latyshev and N. Dolchinkov, "Application of digital telecommunication environment to solve legal issues". Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference. Vol. 2, 2025, [Online]. Available: ETR Journals, <https://journals.rta.lv>. [Accessed: Febr. 14, 2026], <https://doi.org/10.17770/etr2025vol2.8614>
- [8] M. Angelova and A. Zielińska-Chmielewska, "Algorithmic management in the digital transformation of enterprises: A qualitative study of motivations and strategic implications", vol. 9, pp. 79-96, 2025. [Online]. Available: EES Journal, <https://ees.bg>. [Accessed: Mar. 15, 2026], <https://doi.org/10.61954/2616-7107/2025.9.4-6>
- [9] O. Mansour, A. Raslan and N. Ramadan, A Proposed approach for measuring maturity level of software delivery, *Journal of Software Engineering and Applications*, 2024, Vol. 17, pp. 228-245, [Online]. Available: Scientific Research, <https://www.scirp.org/journal/paperinformation?paperid=133291> [Accessed: Mar. 4, 2026], <https://doi.org/10.4236/jsea.2024.175013>
- [10] J. Bumann and M. K. Peter, "Action fields of digital transformation - a review and comparative analysis of digital transformation maturity models and frameworks", In A. H. Verkuil, K. Hinkelmann and M. Aeschbacher, Eds., *Digitalisierung und andere Innovationsformen im Management*, 2019, pp. 13-40. [Online]. Available: FHNW Institutional Repository, <https://irf.fhnw.ch>. [Accessed: Mar. 11, 2026], <https://irf.fhnw.ch/handle/11654/42975>
- [11] E. Omol, L. Mburu and P. Abuonji, "Digital Maturity Assessment Model (DMAM): Assimilation of Design Science Research (DSR) and Capability Maturity Model Integration (CMMI)," *Digital Transformation and Society*, vol. 4, no. 2, 2024. [Online]. Available: Emerald Insight, <https://www.emerald.com/insight>. [Accessed: Febr. 28, 2026], <https://doi.org/10.1108/DTS-04-2024-0049>
- [12] F. Laaber, A. Florack, T. Koch and M. Hubert, "Digital maturity: Development and validation of the Digital Maturity Inventory (DIMI)", *Computers in Human Behavior* vol. 143, 2023. [Online]. Available: ScienceDirect, <https://www.sciencedirect.com>. [Accessed: Apr. 23, 2026], <https://doi.org/10.1016/j.chb.2023.107709>
- [13] T. Thordsen and M. Bick, "A decade of digital maturity models: much ado about nothing?", *Information Systems and e-Business Management*, Vol. 21, Issue 4, pp. 947-976, [Online]. Available: SpringerLink, <https://link.springer.com>. [Accessed: Febr. 10, 2026], <https://doi.org/10.1007/s10257-023-00656-w>
- [14] C. Vilorio-Núñez, F.J. Vázquez and C.M. Fernández-Márquez, "A review of the digital transformation maturity models for SMEs in search of a self-assessment", In Proceedings of the 2022 IEEE Andescon, Barranquilla, Colombia, Nov. 16-19, 2022, [Online]. Available: IEEE Xplore, <https://ieeexplore.ieee.org>. [Accessed: Mar. 23, 2026], <https://doi.org/10.1109/ANDESCON56260.2022.9989889>
- [15] Á. Sándor and Á. Gubán, "A measuring tool for the digital maturity of small and medium-sized enterprises", *Management and Production Engineering Review*, vol. 14, no. 4, pp. 133-143, 2021. [Online]. Available: Polish Academy of Sciences Journals, <https://journals.pan.pl>. [Accessed: Mar. 15, 2026], <https://doi.org/10.24425/mper.2021.140001>
- [16] X. Zheng, "Digital maturity and business model evolution in service firms", *International Journal of Information Systems in the Service Sector*, vol. 16, no. 1, 2025. [Online]. Available: IGI Global, <https://www.igi-global.com>. [Accessed: Febr. 15, 2026], <https://doi.org/10.4018/IJISS.398564>
- [17] E. Omol, P. Abuonji and L. Mburu, "SMEs digital maturity: Analyzing influencing factors and the mediating role of environmental factors", *Journal of Innovative Digital Transformation*, vol. 2, no. 1, pp. 19-36, 2025. [Online]. Available: Emerald Insight, <https://www.emerald.com/insight>. [Accessed: Mar. 9, 2026], <https://doi.org/10.1108/IJDT-01-2024-0002>

- [18] R. Guerrero, C. Lattemann and P. Gebbing, "Helping Personal service firms to cope with digital transformation: evaluation of a Digitalization Maturity Model," *Pacific Asia Journal of the Association for Information Systems*, vol. 15, no. 2, 2023. [Online]. Available: AIS eLibrary, <https://aisel.aisnet.org>. [Accessed: Febr. 13, 2026], <https://doi.org/10.17705/1pais.15201>
- [19] D. Schallmo, K. Lang, D. Hasler, K. Ehmig-Klassen, and C. Williams, "An approach for a Digital Maturity Model for SMEs based on their requirements," *Management for Professionals*, In D. Schallmo and J. Tidd, Eds., Springer, 2021, pp. 87-101. [Online]. Available: SpringerLink, <https://link.springer.com>. [Accessed: Febr. 14, 2026], https://doi.org/10.1007/978-3-030-69380-0_6
- [20] J-I. Jäkel, F. Fischerkeller, T. Oberhoff and K. Klemm-Albert, "Development of a maturity model for the digital transformation of companies in the context of construction Industry 4.0, *Journal of Information Technology in Construction*, vol. 29, pp. 778-809, 2024. [Online]. Available: ITcon, <https://www.itcon.org>. [Accessed: Mar. 17, 2026], <https://doi.org/10.36680/j.itcon.2024.034>
- [21] A. S. I. Tan, B. C. Sia, W. M. Yeong and M. Falahat, "Digital transformation: the role of digital maturity and its determinants on business performance", *Journal of Asia Business Studies*, pp. 1-24, 2025. [Online]. Available: Emerald Insight, <https://www.emerald.com/insight>. [Accessed: Febr. 13, 2026], <https://doi.org/10.1108/JABS-08-2024-0480>
- [22] L. Zhou, Q. Xia, H. Sun, L. Zhang and X. Jin, X. "The role of digital transformation in high-quality development of the services trade", *Sustainability*, vol. 15, no. 5, 2023. [Online]. Available: MDPI, <https://www.mdpi.com>. [Accessed: Febr. 18, 2026], <https://doi.org/10.3390/su15054014>
- [23] K. Z. Chen, I. K. Wang and R. J. Seidle, "Navigating digital transformation: the role of management innovation in achieving digital maturity", *Learning Organization*, vol. 32, no. 3, pp. 391-417, 2025. [Online]. Available: Emerald Insight, <https://www.emerald.com/insight>. [Accessed: Febr. 3, 2026], <https://doi.org/10.1108/TLO-04-2023-0060>
- [24] R. Gurumurthy, D. Schatsky Pivoting to digital maturity, Seven capabilities central to digital transformation, [Online]. Available: Deloitte Insights, <https://www.deloitte.com/us/en/insights/topics/digital-transformation/digital-maturity-pivot-model.html>. [Accessed: Jan. 23, 2026],
- [25] S. Njah, C. Danjou, E. Mosconi, F. Armellini, C. Beaudry, A digital maturity model for assessing SMEs in the manufacturing sector, *Digital Engineering*, Vol. 9, p. 100084, 2026, Available: <https://www.sciencedirect.com/> [Accessed April 3, 2026], <https://doi.org/10.1016/j.dte.2025.100084>
- [26] I.V. Aslanova, A.I. Kulichkina, Digital Maturity: Definition and Model, *Advances in Economics, Business and Management Research*, 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020), vol. 138, 2020, pp. 443-449. [Online]. Available: Atlantis Press, <https://www.atlantis-press.com>. [Accessed: Febr. 17, 2026], DOI:10.2991/aebmr.k.200502.073.
- [27] National Statistical Institute (NSI), "Use of information and communication technologies in enterprises - 2025" (in Bulgarian), 2025. [Online]. Available: NSI, <http://www.nsi.bg>. [Accessed: Apr. 23, 2026].

Applying a Heuristic Approach to Time Optimization in a Grid Schedule

Dimitar Dimitrov

Department of Technology,
Organization and Management of
Transport
Todor Kableshkov University of
Transport, Bulgaria
Sofia 1574, 158 Geo Milev St.
ddimitrov@vtu.bg

Todor Balabanov

Department of Communications and
Electrical Equipment in Transport
Todor Kableshkov University of
Transport, Bulgaria
Sofia 1574, 158 Geo Milev St.
todor.balabanov@vtu.bg

Irena Petrova

Department of Technology,
Organization and Management of
Transport
line 3: Todor Kableshkov University
of Transport, Bulgaria
Sofia 1574, 158 Geo Milev St.
ipetrova@vtu.bg
ORCID: 0009-0001-6321-7210

Abstract— With the development of information technology, the project management process across different sectors of the economy has changed. Very often, new approaches use combinations of familiar, established project management methods to meet the requirements.

This article examines an approach to project management that combines the PERT method and evolutionary algorithms. The goal is to improve the estimate of the possible time required to complete the project. With the PERT method, you can identify the project's critical path and all critical activities. pessimistic, most likely, and optimistic. The project is represented as an acyclic graph, with tasks at the nodes and edges indicating connections between them. Each task is assessed with the three PERT assessments. Combining the two methods results in a shorter critical path, i.e., the time required to complete the project.

Keywords—PERT method, project management, evolutionary algorithm

I. INTRODUCTION

Project management needs adequate tools for planning and optimizing time schedules in the conditions of dynamically changing resources and deadlines. Network graphs provide a visual representation of the logic, sequence, and interdependencies among the project's individual activities. Classical methods for analyzing network schedules, such as the critical path method (CPM) and the program evaluation and review technique (PERT), provide the critical path, early and late deadlines, and time reserves. The methods are effective for relatively small and well-structured projects. They are used as an analysis tool, and additional methods are used to optimize time and resources. [1]

In today's dynamic, high-tech world, managing transport projects requires new methods and software to improve process efficiency and project sustainability.

Solving current problems in the management of transport projects requires an integrated approach that combines methods of system management, the application of innovations and technologies, effective financial planning, and active cooperation among all stakeholders.

Network scheduling optimization tasks solve difficult problems by finding a real-time global optimum and reallocating resources. For this purpose, heuristic and metaheuristic approaches are used to find a good-enough solution for project optimization and resource allocation.

II. INTELLIGENT OPTIMIZATION – EVOLUTIONARY ALGORITHMS

A. Algorithms inspired by nature

Bio-inspired algorithms are gaining great popularity due to their high efficiency and simplicity. There are at least 350 different algorithms of this type, based on over 100 different types and phenomena. Algorithms inspired by:

- Animals (terrestrial, aquatic, flying)
- Natural phenomena (rain, hurricanes, stars, water cycle)
- Music
- Sports
- Inspired by space (black holes), etc. [2]

Evolutionary algorithms (EAs) follow the principles of biological evolution. They are a subset of metaheuristic algorithms. Heuristic algorithms solve problems using readily available information and are based on experience and observation. They are used to support decision-making when exact methods are ineffective. Through them, a good enough solution with practical applicability is found. Metaheuristics are a combination of heuristic approaches to find better solutions. [3]

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.135>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

A characteristic feature of evolutionary algorithms is that they operate not only on a single solution but on a population of solutions. The solutions themselves can be vectors, permutations, or real numbers. Traditional algorithms find local minimum. The evolutionary algorithm using mutation seeks global minimum to achieve better optimization.

Evolutionary algorithms simulate biological processes, making them a powerful tool for finding solutions in large data sets. They search for an optimal solution from a set of potential solutions. In the scientific literature, 5 main types of evolutionary algorithms are identified (Fig. 1).

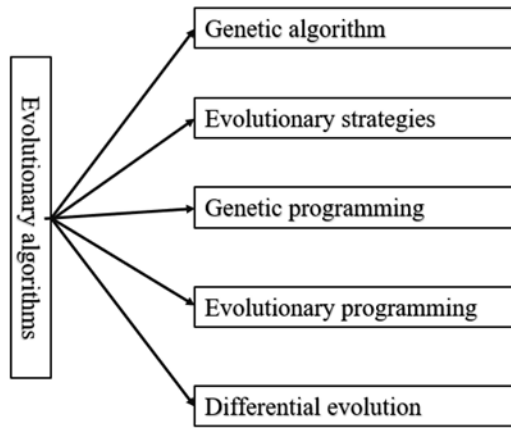


Fig. 1. Types of evolutionary algorithms

What the five main evolutionary algorithms have in common is the way they model processes using biological principles. They work with a population of decisions obtained through selection, mutation, and reproduction [4].

A disadvantage of evolutionary algorithms is the way they identify the optimal solution. The solution produced is the best available at the time. This method is also regarded as slow [5].

B. Program Evaluation and Review Technique /PERT/

The PERT method is a statistical project management tool for analyzing all project work and estimating project duration using three estimates: optimistic, pessimistic, and realistic.

In PERT, each activity is defined by four time estimates: Optimistic—the minimum completion time under ideal conditions;

Pessimistic – the maximum time it can take to complete a task when all anticipated and unforeseen incidents occur.

Most likely, the time is the best estimate of task completion under normal conditions.

As expected, this is the average execution time, as ideal conditions do not exist. It is determined by repeated measurements over time. Formula (1) applies:

$$E = \frac{O + 4 \cdot M + P}{6} \quad (1)$$

where:

O – optimistic assessment;

M – most likely;

P – pessimistic assessment.

The use of these assessments for the project works leads to the development of three scenarios for the project, which can also be visualized in the Gantt chart: pessimistic, realistic, and optimistic. The three assessments provide a more realistic estimate of the project's duration and determine the probability of completion.

$$\text{Variance} = \left(\frac{O - P}{6} \right)^2 \quad (2)$$

Variance calculation from formula (2) reveals risk concerning activity duration. This enables planning for delays in highly volatile tasks.

Defining the critical path enables you to prioritize tasks that could delay the project. Their duration can be reduced by optimizing resources. Identifying critical tasks strengthens risk management. These are the riskiest points requiring a response plan for observed deviations.

The PERT method is usually used in conjunction with the critical path method and in projects with time constraints. The critical path method uses a time and cost limit with one estimate each. In PERT, it does not use costs but three time estimates, and each activity is evaluated using the most likely, pessimistic, and optimistic times. In this way, the management team has information about hazards and the lack of time, based on comparisons of current results with planned results and targets, and on calculations of the probability of achieving the plan.

PERT is used to manage large, complex infrastructure projects. The sequence of application of PERT in the planning of a complex transport project is presented in Figure 2.

A disadvantage of PERT is its complexity in building and maintaining for projects with numerous tasks and connections. Another disadvantage is an excessive focus on deadlines, often at the expense of resources and budget [6].

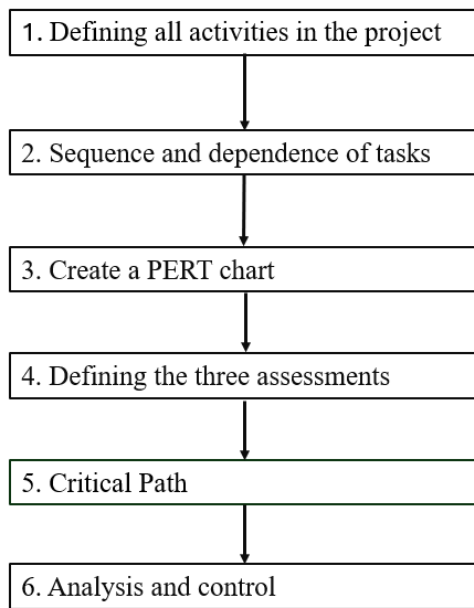


Fig. 2. PERT Step Model

The first step is carried out already at the project planning stage. Determining the sequence and dependencies of tasks is important for tracking them, their deadlines, and the overall duration of the project. Plotting the schedule is the third step. PERT charts visualize the critical path and help estimate task durations and the resources needed. In the fourth step, the three assessments are defined to estimate the most likely project duration. From the schedule and estimates, the project's critical path is determined. In the last step, the critical path is analyzed to determine which tasks can be manipulated to complete the project within the planned deadline.

The PERT diagram shows the sequence of activities that are set when the project is scheduled. Arrows indicate the direction and sequence of activities. The main components of the diagram are the elements: nodes, arrows, and paths. The nodes are depicted as circles or rectangles. They contain information about the duration, name, and resources for the specific task. The arrows illustrate the relationship between the tasks and the possible paths. At the beginning and end, dummy events with zero duration can be added [7].



Fig. 3. PERT chart

One drawback of the PERT chart is its dependence on expert judgment, which, if inaccurate, may lead to significant project consequences. Fig. 3 presents a sample PERT chart created with canva.com. The diagram indicates that executing activity D002 will likely require 3 days. It is estimated to take 2 days or, in the event of issues, up to 4

days. The average duration of the activity, calculated using formula 2, is 3 days [8].

III. MATERIALS AND METHODS

A. Mathematical Statement

The presented PERT-EA model addresses the management of a transport project by combining the well-known PERT approach with an evolutionary algorithm. The purpose of the model is to provide a more acceptable estimate of the project's possible duration. The PERT method provides an expected time range for completing the project, using three types of assessments: pessimistic, optimistic, and most likely. With it, the critical path can be found. When constructing a project graph, the work is placed in the nodes.

The transport infrastructure project is presented as a network of activities.

Let project W be a set of activities:

$$W = \{A, B, C, \dots\} \quad (3)$$

As with A, B, C..., the activities are indicated in the column for clearer writing.

Each activity is characterized by three times:

mi – average duration of the activity

AI – Optimistic assessment of the duration of the activity

BI – pessimistic assessment of the duration of the activity

The average duration is the constant element. Optimistic and pessimistic estimates can vary. It is unwise to alter the average estimate, as it is typically derived from empirical experience and precise measurements.

The expected estimate shall be calculated according to the known formula (4).

$$t_i = \frac{a_i + 4 \cdot m_i + b_i}{6} \quad (4)$$

where i is the project's activity number.

The network schedule for the AON-type project is drawn. In the vertices of the column are the names of the works, and the weights along the arcs are time estimates. Two auxiliary (service) vertices are entered, corresponding to the project's beginning and end. The graph is necessary to describe all possible paths for the project and all connections between the individual activities.

When creating the network schedule, Table I is used. Timely completion of the project depends on the resource management approach, one of which is time itself. 6 (six) main parameters are used for time management:

- RS – Early start
- RK – Early End
- CS – Late start
- CC – Late End
- P – Duration

- P – reserve.

Reserves are calculated for each activity. Critical activities with zero reserve are flagged. Optimization can assess activities along possible paths in the network schedule by adding resources such as equipment, funding, or personnel.

When creating a PERT graph, Table I is filled in two passes: a straight pass and a reverse pass. The duration column receives the weighted estimate for activity t_i from formula 4. The early-start cell records the result from formula (5).

$$PC = \max (RC \text{ of previous activities}) \quad (5)$$

Record the early end using formula (6).

$$RK = P + RS \quad (6)$$

In the reverse pass, the column is traversed from the end to the beginning, and the third row of Table I is filled in. In the last cell, the result of formula (7) is filled in.

$$CC = \min (CC \text{ of previous works}) \quad (7)$$

In the Late start cell, enter the value obtained from formula (8).

$$KS = KK - P \quad (8)$$

In cell Reserve, enter the difference between late end and early end using formula (9).

$$P = CC - RK \quad (9)$$

TABLE I. PERT SCHEDULE PRINCIPAL TIME

Early start	Duration	Early End
Name of activity		
Late start	Reserve	Late end

The target function takes the form of equation (10).

$$\min T_j = f(a_i, b_i) \quad (10)$$

such as:

a_i is a vector of optimistic assessments

b_i is a vector of pessimistic assessments.

One disadvantage of the PERT method is the reliance on expert assessments. In this case, this disadvantage is used as the average score (m_i) is taken from the MS Project, and conditions and limits are set for the optimistic and pessimistic ones.

Several types of target function models are tested to find the most acceptable one that minimizes the objective, with the Solver adjusting the optimistic and pessimistic estimates.

To find the minimum total time, the Solver tool in MS Excel is applied. Each solution represents a distinct scenario, and the decision-maker selects the preferred option.

The restrictions are:

1. $a_i > 0$
2. $a_i \leq m_i$
3. $b_i \geq m_i$
4. $a_i \geq k_a * m_i$
5. $b_i \leq k_b * m_i$

B. Algorithm for the implementation of PERT – EA

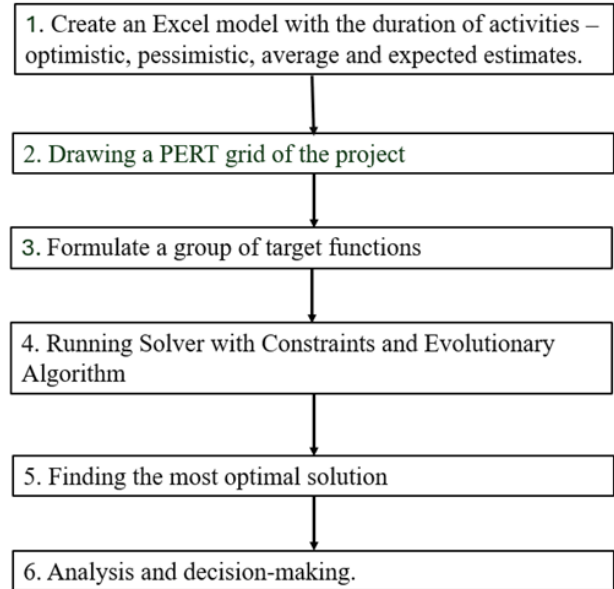


Fig. 4. PERT-EA application algorithm

Fig.4 shows the sequence and specific steps in applying the PERT-EA method.

C. Solver module

A Solver module is available in MS Excel, which has a built-in Evolutionary optimizer. This optimizer uses evolutionary algorithms without guaranteeing reaching a global optimum, but gives good chances for reaching sub-optimal solutions. Parameters (settings) are set in advance, and the resulting solution is returned.

In order for the Solver to stop working and give a solution, one of the conditions must be met:

- The set heuristic rules state that no significant improvement is expected in the next iteration.
- The set time limits have been exceeded. The number of trial solutions has been reached.

From the Solver Parameters – Options dialog box, additional settings can be made to the Evolutionary Solving Method. The correct selection of parameters is an essential decision on the effectiveness of the optimization.

Convergence – a maximum allowable percentage difference in the values of the target function is introduced for the best 99% of the solutions. Lower convention values lead to more precise results, but increase the calculation time.

Mutation Rate – enter a number in this field – relative frequency in the range [0; 1]. The number indicates how a member of the population will mutate to create a new trial solution. A higher frequency value increases the diversity of the population and improves the likelihood of finding a better solution.

Population Size – enters the number of solutions viewed at the same time. The minimum value is 10. If no value is set, Solver automatically sets the size to a value between 10 and 200.

Random Seed – A positive integer is entered. This parameter gives the starting value for generating random numbers. If the field is empty, random values are used, which can lead to different decisions on each start.

Maximum Time without Improvement – the maximum time during which the algorithm can work without a significant improvement to the best solution is introduced.

Require Bounds on Variables – checking this box sets the lower and upper execution limits [9].

IV. RESULTS AND DISCUSSION

In the created model, five target functions are considered and tested to find a solution that best meets the decision-maker's needs. The model allows decision-makers to better navigate the optimistic and pessimistic phases of implementing project activities.

The input data is taken from Solver and used in the solution. They are the basis for calculations of the expected time. They compare durations and identify and identify bottlenecks [10].

Target function T1 is linear, calculated using formula (10), and serves as a reference function. Table II contains the solution obtained with Solver for the target function T1. The PERT graph (Fig. 5) gives the dependencies between the project activities. For target function T1, the critical path includes the activities $S \rightarrow B \rightarrow E \rightarrow G \rightarrow K \rightarrow O \rightarrow Z$. The longest activities are K (8.67), H (7.80) and I (6.94). The shortest activities are A (2.60) and M (2.60). The expected time to complete the project is 26.87. All activities on the critical path have zero reserve. Non-critical activities have a positive reserve and can be shifted without changing the deadline, for example, activity I can be shifted by about 6.06 and activity N by about 4.34.

The evolutionary algorithm represents each solution as a chromosome, where genes encode estimates of the pessimistic and optimistic times for activities within the defined limits. When starting the Solver, the target function values for time, reserves, and load are determined. The algorithm uses the initial population to evaluate solutions, selects the better ones, combines them, and introduces mutations in the form of random values.

TABLE II. TABLE TYPE STYLES

	<i>Optimistic</i>	<i>Ka*_m</i>	<i>Realistic</i>	<i>Kb*_m</i>	<i>Pessimistic</i>	<i>Expected</i>
<i>Work</i>	<i>a</i>	<i>0,8*_m</i>	<i>m</i>	<i>1,2*_m</i>	<i>b</i>	
A	2.40	2.4	3	3.6	3.00	2.90
B	3.20	3.2	4	4.8	4.00	3.87
C	4.00	4	5	6	5.00	4.83
D	5.62	5.6	7	8.4	7.03	6.77
E	4.81	4.8	6	7.2	6.01	5.80
F	4.02	4	5	6	5.01	4.84
G	4.01	4	5	6	5.00	4.84
H	7.21	7.2	9	10.8	9.00	8.70
I	6.44	6.4	8	9.6	8.01	7.74
J	3.21	3.2	4	4.8	4.01	3.87
K	8.01	8	10	12	10.01	9.67
L	6.40	6.4	8	9.6	8.04	7.74
M	2.41	2.4	3	3.6	3.01	2.90
N	5.61	5.6	7	8.4	7.01	6.77
O	4.80	4.8	6	7.2	6.00	5.80

With each generation of a new chromosome, there is a change in times. In the critical pathway, a new total duration is obtained.

The algorithm stops when it has found a stable optimal solution, meaning a well-balanced schedule, a minimum critical path, and optimal use of reserves.

A Solver is applied to each target function, resulting in changes to the input data and the network schedule's critical path.

The solution obtained with Solver for target function T2 yields a highly modified network graph. The critical path of the project is: $S \rightarrow B \rightarrow E \rightarrow H \rightarrow N \rightarrow Z$, with a duration of 59.82. The optimization has led to a large increase in time. The longest activities are N (25.04) and E (22.98), and the shortest B (4.00) and H (7.80).

The solver receives upper and lower bounds on the ratings a_i and b_i , which we set in the coefficients k_a and k_b . The coefficient k_a determines the lower limit of the assessment a_i , and k_b determines the upper limit of b_i . The assessment of AI should not be negative..

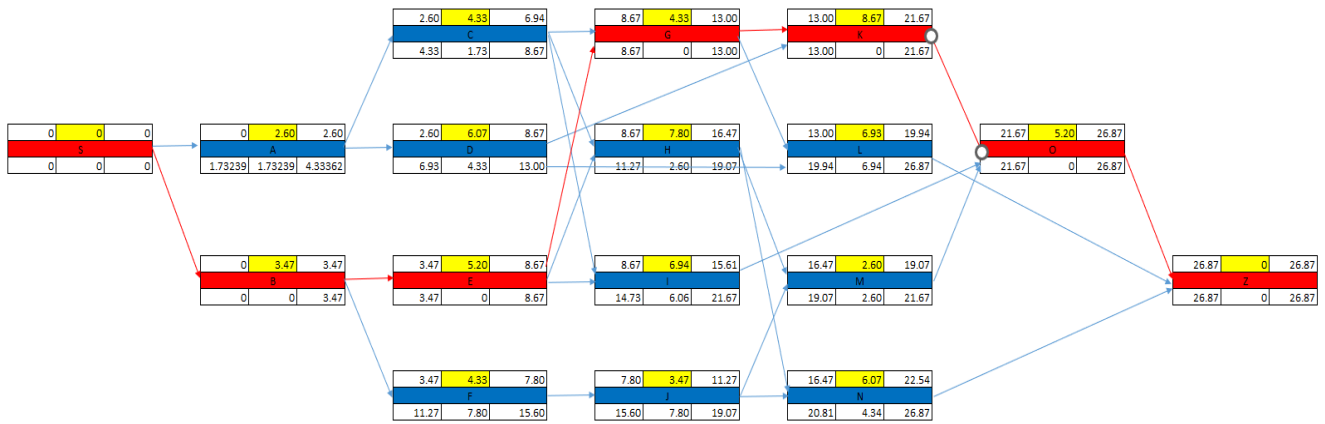


Fig. 5. PERT charter of Target function T1

The critical pathway for target function T3 is $S \rightarrow A \rightarrow D \rightarrow K \rightarrow O \rightarrow Z$, with a duration of 58.51. There is a slight decrease in the critical pathway compared to that of T2. The longest critical activities are D (22.89) and K (22.76). The shortest activities are O (5, 20) and A (7.66).

The critical path for target heading T4 includes the activities: $S \rightarrow A \rightarrow C \rightarrow G \rightarrow K \rightarrow O \rightarrow Z$. The project is expected to be completed in a possibly shorter period compared to target headings T2 and T3 with an output of 34,31. The longest activity for heading T4 is A (11, 75) and the shortest duration is C (4,34) and G (4,34).

For target function T5, the critical path includes the following activities $S \rightarrow B \rightarrow F \rightarrow J \rightarrow M \rightarrow O \rightarrow Z$ with a duration of 33,41. This is the second most preferred estimate of time after the decision obtained under target function T1. The longest critical activity is F (18,63) and the shortest activity is M (2,61).

TABLE III. SUMMARY DATA

Target function	Table Column Head		
	Critical Path	Longest critical activity	Shortest critical activity
T1	$S \rightarrow B \rightarrow E \rightarrow G \rightarrow K \rightarrow O \rightarrow Z$	K (8.67)	A (2,60) M(2,60)
T2	$S \rightarrow B \rightarrow E \rightarrow H \rightarrow N \rightarrow Z$	N (25,04)	B (4,00)
T3	$S \rightarrow A \rightarrow D \rightarrow K \rightarrow O \rightarrow Z$	D (22,89)	O (5, 20)
T4	$S \rightarrow A \rightarrow C \rightarrow G \rightarrow K \rightarrow O \rightarrow Z$	A (11, 75)	C (4,34) G (4,34)
T5	$S \rightarrow B \rightarrow F \rightarrow J \rightarrow M \rightarrow O \rightarrow Z$	F (18,63)	M (2,61)

Table III presents the aggregated data on critical pathways after a solution with Solver.

The proposed approach to pessimistic and optimistic assessment provides different scenarios for the project's course, especially regarding the formation of activities on the critical path. This variety of scenarios provides additional opportunities for making well-reasoned decisions.

V. CONCLUSIONS

The authors thank their affiliated institutions for their support of this research. They also appreciate the helpful discussions and technical insights that shaped this work.

VI. ACKNOWLEDGMENT

The authors thank their affiliated institutions for their support of this research.

REFERENCES

- [1] D. Nikolova and M. Lazarova, Metaheuristic optimization methods in resource planning and business process management, Automation and Informatics, https://sai-bg.com/wp-content/uploads/2021/08/6-paper-6-D.Nikolov_M.Lazarova-pages-34-44-AI-3-2019.pdf 2019.
- [2] S. Darvishpor, A. Darvishpour, M. A. Escarcega and M. Hassanalian, Nature-Inspired Algorithms from Oceans to Space: A Comprehensive Review of Heuristic and Meta-Heuristic Optimization Algorithms and Their Potential Applications in Drones, Drones, 7(7):427, DOI: [10.3390/drones7070427](https://doi.org/10.3390/drones7070427), 2023.
- [3] R. Marti, P. Panos and M. G. C. Resende, Handbook of Heuristics, Springer International Publishing, eBook ISBN 978-3-032-00385-0, <https://doi.org/10.1007/978-3-032-00385-0>, 2025.
- [4] P. Georgieva, "Genetic Algorithms as a Tool for Solving Optimization Problems", Computer Sciences and Communications, Vol. 2 No. 3, <https://csc.bfu.bg/index.php/CSC/en/article/view/172> 2013.
- [5] "Genetic Algorithms and Evolutionary Algorithms – Introduction", Frontline Solvers, 06.01.2024. [Online]. Available: <https://www.solver.com/genetic-evolutionary-introduction>. [Accessed: 29. 05, 2026].
- [6] A. Team, "PERT chart: Definition, Examples & How to Make One," Asana, 14 01 2026. [Online]. Available: <https://asana.com/resources/pert-chart> [Accessed 29 05 2026].
- [7] "Programme Evaluation and Review Technique (PERT)," [Online]. Available: <https://www.ifm.eng.cam.ac.uk/research/dstools/pert/> [Accessed 24 04 2026].
- [8] L. Roux, "What is a Pert chart?" Wimi, 25 03 2026. [Online]. Available: <https://www.wimi-teamwork.com/en/blog/project-management/pert-diagram> [Accessed 25 04 2026].
- [9] "Excel Solver - Change Options for Evolutionary Solving Method," Frontline Systems, [Online]. Available: <https://www.solver.com/excel-solver-change-options-evolutionary-solving-method> [Accessed 24 04 2026].
- [10] D. Dimitrov, T. Razmov, "Manual for Laboratory Exercises and Course Design in Project Management", Sofia: Todor Kableshkov University of Transport, 2012.

Cybersecurity Threats in Intelligent Transport Systems: Challenges and Solution Pathways

Dimitar Dimitrov

Faculty of Transport Management
University of Transport
Sofia, Bulgaria
ddimitrov@vtu.bg

Krassimir Lalov

Faculty of Transport Management
University of Transport
Sofia, Bulgaria
klalov@vtu.bg

Ivan Manchev

Faculty of Transport Management
University of Transport
Sofia, Bulgaria
imanchev@vtu.bg

Irena Petrova

Faculty of Transport Management
University of Transport
Sofia, Bulgaria
ipetrova@vtu.bg

Abstract— The rapid integration of Intelligent Transport Systems (ITS) into urban and interurban mobility has significantly improved efficiency, safety, and automation in transport operations. Nevertheless, the extensive connectivity enabled by vehicle-to-everything (V2X) communications, Internet of Things (IoT) devices, and cloud services has also increased exposure to cyber threats. The primary scientific challenge is that compromising Cooperative ITS (C-ITS) can enable manipulation of critical transport functions, such as automated control, braking, and signaling, through falsified or maliciously injected communication messages. The increasing frequency of distributed denial-of-service (DDoS) attacks exacerbates this vulnerability, as these attacks account for most publicly recorded incidents worldwide and directly affect the transportation sector. Furthermore, ransomware and supply-chain attacks have led to a marked increase in system breaches and significant financial losses.

IoT devices widely deployed within ITS often use inadequately secured communication protocols, creating opportunities for remote intrusion and infrastructure compromise. Simultaneously, Artificial Intelligence (AI) functions as a dual-use technology, facilitating both cyber-attacks, such as automated phishing, adaptive threat generation, and vulnerability analysis, and defense through the deployment of anomaly detection models. Additional risk arises from adversarial attacks that can mislead AI models in autonomous vehicles, thereby undermining real-time decision-making processes.

Proposed solutions include integrating international standards, such as ISO/SAE 21434 and the NIST Cybersecurity Framework; applying cryptographic

protection to V2X communications; implementing hybrid intrusion detection systems; and adopting lifecycle-oriented risk management across ITS infrastructures. AI-based predictive analytics and anomaly detection are identified as critical approaches to enhancing cyber resilience. Ongoing coordination among operators, vendors, and public institutions is essential to mitigate systemic risks and protect the integrity of ITS environments.

Keywords—Intelligent Transport Systems, Cybersecurity Threats, Internet of Things (IoT), vehicle-to-everything (V2X), Artificial Intelligence.

I. INTRODUCTION

Intelligent Transport Systems (ITS) integrate digital, communication, and control technologies to enhance the safety, efficiency, and sustainability of transportation. Modern ITS operates as a complex cyber-physical system, combining the Internet of Things (IoT), vehicle-to-everything (V2X) communications, and Artificial Intelligence (AI) to collect and process large volumes of real-time data. While this digitalization improves transportation infrastructure, it also introduces unpredictable cybersecurity threats that may seriously impact public safety and critical infrastructure [1], [2].

The rapid growth of IoT devices in intelligent transport systems, including smart sensors, road infrastructure, on-board computers, and edge network elements, significantly expands the attack surface. Heterogeneous devices, limited computing resources, and the lack of standardized defense mechanisms make these systems particularly vulnerable to threats that compromise data integrity, privacy, and

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.138>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

availability. Studies indicate that traditional cryptographic methods often fail to address modern threats such as distributed denial-of-service (DDoS) attacks, data tampering, malicious device management, and zero-day attacks in large-scale IoT environments [3], [4].

Vehicle-to-everything (V2X) communications are critical to cybersecurity. V2X enables vehicles, infrastructure, pedestrians, and network services to exchange information, supporting automated traffic management, incident prevention, and autonomous transport. However, V2X remains vulnerable to attacks such as spoofing, Sybil, replay, and route manipulation, which can disrupt real-time decision-making and lead to physical incidents. Literature reviews highlight the lack of unified security architecture and effective trust management as major challenges for V2X systems [5], [6].

Artificial intelligence is becoming a key tool for strengthening the cyber resilience of ITS. Techniques such as machine learning, deep neural networks, and federated learning support anomaly detection, trust management, attack prediction, and automated incident response. Studies indicate that AI significantly improves detection of complex, adaptive attacks in dynamic transport networks, where static defenses are often insufficient [7], [8].

Although significant progress has been made, integrating artificial intelligence into Intelligent Transport Systems (ITS) cybersecurity poses challenges related to model interpretability, data quality, and resilience to adversarial attacks. Addressing these issues requires a comprehensive, interdisciplinary strategy that incorporates technological, architectural, and managerial solutions. Consequently, systematic research into cybersecurity threats within Intelligent Transport Systems is crucial for developing reliable, safe, and sustainable transport services amid ongoing digital transformation [1], [9].

II. ITS WORKING MODEL

ITS is vital for efficient transportation infrastructure, improving road safety, and reducing environmental impact. By integrating IoT, big data, and artificial intelligence, ITS processes large volumes of data in real time to optimize traffic, monitor road conditions, and support vehicle-to-infrastructure communication. However, increased reliance on digital technologies also raises the risk of cyberattacks, technical failures, and network anomalies. To better understand ITS operations and protection strategies, it is helpful to review the Intelligent Transport System model, which includes three main components: the ITS architecture level, the integrated management level, and the ITS security levels [2]. Formula 1 and Figure 1 present this model.

$$\text{ITS Working Model} = f(\text{Integrated Management Level}, \text{ITS Architecture Level}, \text{ITS Security Level}) \rightarrow \max \quad (1)$$

A. Integrated Management Level

This component comprises two modules: the Analytical Level and the Management and Integration Level. The Analytical Level processes large volumes of data from sensors and communication systems using advanced machine learning algorithms. It analyzes both structured

and unstructured data, including video streams, sensor signals, and event logs, to detect anomalies and support transport optimization decisions.

Key functions include analyzing historical and real-time data to predict scenarios such as traffic congestion, adapting system behavior, optimizing resource allocation, detecting abnormal activity, and modeling risks related to weather, accidents, or cyberattacks. The Analytical Level works closely with the Computing Layer, which supplies processed data, and the Management Layer, which uses analytical results to inform decisions. For example, traffic forecasts can be sent to traffic light control systems for dynamic adjustments or provided to drivers through user interfaces.

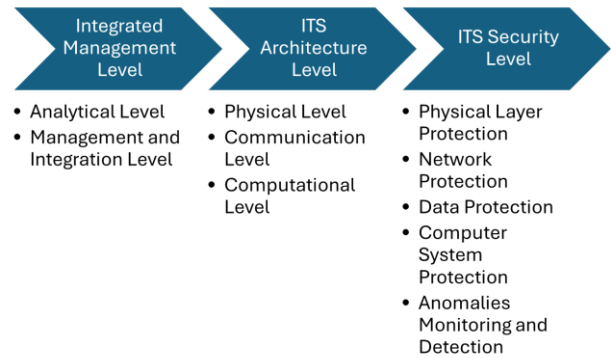


Fig. 1. ITS Working Model

The Management and Integration Level coordinates interactions among users, control systems, and infrastructure components, enabling real-time strategic management of the transport network. Its primary role is to synchronize all system components to optimize efficiency, safety, and convenience. This layer aggregates data from the physical, communication, computing, and analytical layers to formulate and implement optimization decisions. For example, if traffic increases in a specific area, the system can reroute vehicles to alternative routes.

The Management Layer also integrates with other infrastructure elements: it manages charging stations and electric-vehicle energy consumption, transmits data to emergency services during incidents, and monitors vehicle emissions to minimize environmental impact. Effective governance and integration are essential to building reliable, adaptable transport systems that operate efficiently in complex urban environments.

B. Architecture Level

The physical layer forms the foundation of the ITS architecture, encompassing infrastructure such as roads, bridges, tunnels, traffic lights, parking meters, sensors, and IoT devices [10]. This layer collects data on traffic flows, road conditions, and weather. IoT devices are essential for continuous monitoring and data transmission. For example, traffic sensors measure flow and speed, weather sensors monitor environmental conditions, GPS trackers provide real-time vehicle positioning, and video cameras assess traffic conditions and detect violations or emergencies.

The physical layer also interacts with other system layers. Traffic sensors and signals can adjust in real time based on traffic volume, while V2I technologies provide vehicles with traffic, accident, and speed-limit information. Key challenges at this level include ensuring the reliability of IoT devices under adverse conditions [11], maintaining comprehensive real-time monitoring, and protecting against physical attacks or unauthorized access.

Data collected at this layer is transmitted to the communication layer for processing, and video streams are analyzed at the analytical layer to detect violations. This information supports management decisions on traffic optimization and emergency response. The communication layer enables data transfer among all ITS components. Its goal is to provide efficient, reliable, and secure information exchange among physical devices, computing centers, and users, using wireless protocols (Wi-Fi, 5G, V2X), fiber-optic lines, and satellite systems [12].

This layer enables low-latency, real-time data exchange, transmitting information from traffic lights, sensors, and vehicles for processing and analysis. It integrates technologies via protocols such as V2X for data exchange among vehicles, infrastructure, pedestrians, and cloud platforms; 5G for high bandwidth and minimal latency; and fiber-optic networks for high-speed transmission between data centers.

Challenges include minimizing transmission delays, securing data against interception or tampering, and supporting diverse devices and protocols with varying technical standards. Reliable communication is essential for system coordination and underpins the analytics and control layers. Fast, accurate data exchange enables machine learning algorithms to detect anomalies or predict congestion and provides users with current traffic information.

The computational layer provides the system's processing power, including servers, cloud platforms, and data centers where collected data is analyzed. It runs artificial intelligence algorithms for traffic prediction and resource management. Sensor data, such as vehicle speed and road conditions, is sent to computing platforms for rapid analysis, and results are delivered to the analytical layer or directly to control devices. Machine learning and AI algorithms at this level support traffic flow analysis, congestion prediction, and emergency detection. The computational layer links the physical, communication, and analytical layers by receiving, processing, and transmitting data for further analysis.

C. Security Level

Intelligent transport systems are vulnerable to cyberattacks and technical failures, making multi-layered protection essential. Key protection levels include: Physical Layer Protection, which secures equipment and sensors and restricts access to authorized personnel through surveillance and other measures; Network Protection, which employs firewalls, VPNs, traffic encryption, and secure communication protocols such as V2X to prevent unauthorized access and mitigate DDoS risks; Data

Protection, which uses encryption, user authentication, and access controls to reduce data leakage and privacy breaches; Protection of Computer Systems, which involves regular software updates, server monitoring, intrusion detection systems, and cloud security through access controls and backup policies; and Anomaly Detection, which uses real-time algorithms to identify and respond to suspicious network activity. To assess risks and maintain ITS stability, probabilistic mathematical models estimate the likelihood of threats and anomalies. These models incorporate historical and current data, supporting accurate prediction of potential issues. Estimating the probability of cyberattacks relies on threat probability functions that account for time-dependent risks. Exponential and Weibull distributions help model both constant and changing risks, reflecting factors such as vulnerability accumulation or the impact of security measures. Anomaly detection in network traffic is also critical, using machine learning algorithms and Bayes' theorem to estimate the probability of anomalies based on current traffic patterns. This approach considers both normal and abnormal system behavior. Integrating these methods into the monitoring process enables a comprehensive security system that addresses both global risks, such as cyberattacks, and local network anomalies. This is increasingly important as the complexity of ITS and the number of connected devices continue to grow.

D. Challenges to the development of ITS

As intelligent transport systems grow more complex, real-time data processing becomes essential. Effective threat-response automation requires coordination among ITS components, including traffic control centers, self-driving vehicles, and infrastructure sensors. Machine learning algorithms detect deviations from normal behavior, which is vital for preventing cyberattacks. Reliable data and robust cybersecurity protocols are crucial for system reliability. Current ITS cybersecurity relies on hybrid models that integrate statistical methods, machine learning, and predictive analysis. Ongoing research should further develop these models and algorithms to strengthen risk management and cybersecurity in ITS.

III. ITS CYBERSECURITY THREATS AND REQUIREMENTS

Intelligent Transport Systems integrate IoT devices, V2X communications, and AI-based controls, introducing a range of cybersecurity threats. Recent literature typically classifies these threats using a functional-architectural approach:

TABLE I. CLASSIFICATION OF CYBERSECURITY THREATS IN ITS

Layer / Component	Threat Type	Description and Impact	Ref
IoT layer	Device compromise	Insufficiently secured sensors and edge devices enable unauthorized access, data tampering, and malware injection	[3], [4]

	Botnet / DDoS attacks	Large-scale compromise of IoT nodes used to launch denial-of-service attacks against transport services	[2]
V2X communications	Spoofing and Sybil attacks	Injection of falsified messages and identities, leading to incorrect safety and traffic management decisions	[5], [6]
	Replay attacks	Re-transmission of legitimate V2X messages to manipulate vehicle and infrastructure behavior	[5]
Network layer	Man-in-the-Middle (MitM)	Eavesdropping and manipulation of data exchanged between vehicles and infrastructure	[5]
Application layer	Data injection attacks	Manipulation of input data used by traffic control systems and AI-driven decision mechanisms	[7]
AI components	Adversarial attacks against models	Malicious inputs designed to mislead AI models and cause incorrect predictions or control actions	[8]
	Data poisoning	Intentional contamination of training datasets degrades the performance and reliability of AI systems	[7]
System level	Privacy breaches	Leakage of sensitive location and personal data of transport system users	[1], [3]

Table 1 shows that cybersecurity threats in ITS can cause physical and safety-related impacts, not just digital consequences. This distinguishes Intelligent Transport Systems from traditional IT infrastructure.

A. Emerging V2X Applications and Challenges

V2X systems exhibit certain peculiarities in deployment options and data traffic characteristics compared with traditional network applications.

TABLE II. V2X APPLICATION CATEGORIES AND ASSOCIATED QOS REQUIREMENTS.

Application	Use cases	Connectivity mode(s)
Road safety	•Collision warning Road safety •Vehicle status warning •Vehicle type warning	V2V, V2I
Traffic management	•Speed limit notification •Vehicle tracking •Traffic flow control	V2I, V2N
Comfort and infotainment	•In-vehicle Internet access •Point of interest alerts •Parking booking	V2I, V2N
Autonomous driving	•Advanced driving •Remote driving •Vehicle platooning	V2V, V2I V2N V2V, V2I

V2X systems span a wide range of network scenarios and support vehicular services with diverse QoS requirements. Specifically, four prevalent classes of emerging V2X applications can be identified within the ITS domain: road safety, traffic management, comfort and infotainment, and autonomous driving, as defined in [13].

Table II outlines the main V2X application categories and example use cases for each. Latency, data rate, and message transmission reliability are key performance indicators (KPIs) for road safety and mobility applications.

B. Security and Privacy Requirements

The primary goal of V2X communication systems is to improve road safety and traffic flow by facilitating targeted information exchange between vehicles and road infrastructure. In safety-critical situations, event-driven warning notifications (such as DENMs or BSMs) are activated to alert drivers, and authorized users must reliably access these notifications. The receiving vehicle must confirm that the message originates from an authentic source. These mechanisms emphasize three fundamental security elements: availability, message integrity, and authenticity [14]. Security risks, such as compromised vehicles transmitting fabricated alerts or adversaries generating counterfeit messages, can seriously impair system operation. These risks are particularly significant in V2X scenarios within C-ITS, including vehicle platooning, cooperative collision avoidance, dynamic map dissemination, and remote driving. Attacks against V2X communication protocols like IEEE 802.11p and C-V2X are increasingly sophisticated [15], [16], [17]. Therefore, it is essential to fulfill critical security and privacy requirements to sustain a secure ITS environment and reduce cybersecurity vulnerabilities. These requirements may differ depending on the sensitivity of the ITS application [18] and the tactics employed to counter specific threats. The subsequent sections deliver a concise summary of V2X security and privacy requirements.

Authentication: This process distinguishes legitimate entities from malicious ones in V2X communication and verifies the sender's identity. This enables unique participant identification and verification [19]. The process comprises user authentication, which confirms device legitimacy, and message authentication, which ensures messages originate from valid sources and remain unaltered.

Authorization: This function manages access to V2X services, ensuring that only verified entities receive the appropriate privileges. Authorization is governed by explicit rules and policies that control access to designated services.

Availability: This guarantees authorized users have continuous access to V2X messages and services. Availability safeguards system operation during disruptions, such as denial-of-service attacks, so authorized entities can access the network without interruption.

Confidentiality: This restricts access to V2X message content to designated recipients, preventing unauthorized interception. Confidentiality is commonly delivered through encryption with shared keys. Although most V2X data is public and does not demand strict confidentiality [20], it is vital to prevent data correlation that might expose user identity or location.

Integrity and Data Trust: This upholds the exchange of accurate, consistent, and promptly verifiable information among V2X entities. V2X systems must deploy

mechanisms that uncover and block data manipulation by malicious actors.

Privacy: Safeguarding V2X user identities prevents vehicle tracking and protects sensitive information. Exposing private data can enable systemic attacks and jeopardize user assets. Privacy can be preserved through anonymization or data obfuscation [21], such as assigning vehicles pseudonyms to conceal their identities. Additional privacy requirements, including anonymity, unlinkability, and unobservability, must be maintained through rigorous security practices and policies [20].

vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N).

B. Attacker Model Overview

Attack detection systems are typically designed to identify specific attack types and assess detection performance. Therefore, a comprehensive understanding of attacker behavior and associated attack types is essential for implementing resilient defense mechanisms.

Threats to V2X networks

Authentication	Availability	Confidentiality	Integrity	Privacy
• Sybil • Impersonation • GPS spoofing • Free-riding	• Denial-of-service • Jamming • Flooding • Spamming • Malware	• Eavesdropping • Traffic analysis • Man-in-the-middle	• Modification • Replay • Masquerade • Illusion	• Location tracking • Identify revealing

IV. SECURITY THREATS AND ATTACKS OTHER

This section presents a comprehensive analysis of threats and attacks that can compromise V2X networks, along with a classification of malicious attacks documented in the literature.

A. Attack Surface Overview

The attack surface comprises all potential vulnerable entry points that may compromise the security of a V2X system and serve as sources for adversarial attacks or malicious incidents. Examples include in-vehicle user devices such as USB, Wi-Fi, and Bluetooth within infotainment systems, as well as vehicle sensors. As vehicle automation advances, the number of electronic components in in-vehicle networks increases, expanding the attack surface for elements such as electronic control units (ECUs) and the control area network [22]. The study in [23] systematically analyzes various threat vectors within vehicles, including Bluetooth, cellular, WiFi, and RFIDs, and experimentally demonstrates that in-vehicle ECUs are susceptible to remote attacks. The deployment of cooperative intelligent transport systems (C-ITS) further increases interconnection with the external environment, including other vehicles, roadside units (RSUs), and pedestrians, through V2X technologies. As a result, in-vehicle network components are increasingly exposed to external threats. In Internet of Vehicles (IoV) environments, attack surfaces can be categorized into three domains [24]: in-vehicle, V2X access, and infrastructure. Certain attack types, such as denial-of-service (DoS) and flooding, may affect all three domains, while others, such as tampering or physical damage, are specific to a single domain. V2X communication is a primary target for IoV security attacks, including eavesdropping, communication hijacking, spoofing, data injection, and impersonation. Therefore, this paper focuses on the V2X access domain, which encompasses all V2X connectivity modes, including

Fig. 2. Classification of V2X cybersecurity threats according to compromised security and privacy requirements.

Currently, there is no universally accepted model for classifying V2X attack variants. This analysis adopts the attacker model proposed in [25], which systematically defines the capabilities and methods available to attackers targeting assets such as vehicles, roadside units (RSUs), and communication channels. According to [25], an attacker is classified as an insider when they possess valid credentials that allow communication with legitimate system members or provide system-wide access. These authenticated insiders generally adhere to system protocols but may transmit false or fabricated information. In contrast, attackers without valid credentials or system access are considered outsiders. Outsiders, also known as intruders, have limited capabilities to launch attacks but can eavesdrop on communication links and infer sensitive information, such as security keys or user data. Attackers may also be categorized as malicious or rational based on their intent. Malicious attackers seek to disrupt or harm legitimate users and destabilize system functionality, often disregarding costs or consequences (e.g., causing accidents, denial-of-service (DoS) attacks, or traffic congestion). Rational attackers, by contrast, are motivated by personal gain, such as financial incentives or insurance fraud, and their methods and targets are often more predictable. V2X attacks can be further distinguished by execution mode: active or passive. Active attackers engage directly with the system, transmitting malicious packets or signals through V2X channels. Representative active attacks include DoS, message replay, false data injection, man-in-the-middle (MitM), and Sybil attacks. These are generally considered the most frequent threats to vehicular networks [6]. Passive attackers, on the other hand, primarily eavesdrop on communications to infer critical information, such as certificates, private keys, or user data, without direct interaction.

C. Classification of Attacks

A variety of existing studies have investigated security threats in the context of V2X communication [16], [26]. These works categorize attacks based on factors such as the wireless interface, communication scope, and behavioral characteristics, thereby aiding the development of robust security solutions for vehicular services. This section elaborates on security threats and attacks that are both common and effective against V2X networks. The classification, summarized in Figure 2, is based on key security requirements: authentication, availability, confidentiality, data integrity, and privacy. While each attack is classified under a primary security requirement, certain attacks, such as malware, may compromise multiple requirements simultaneously. Table 5 summarizes the key characteristics of various attacks in V2X networks, including the feasibility of launching each attack and the associated severity, particularly in safety-critical scenarios. Attacks that significantly impact operational performance or result in privacy breaches are categorized as high severity [27]. Relevant references indicate which communication technologies are susceptible to specific attacks or threats.

These examples demonstrate that many attacks effective against conventional communication systems remain highly effective in V2X environments.

V. PROACTIVE SECURITY MECHANISMS IN VEHICLE-TO-EVERYTHING (V2X) COMMUNICATION

Proactive security mechanisms serve as the primary defense in Vehicle-to-Everything (V2X) communication systems, aiming to prevent cyberattacks before they affect system operations. Unlike reactive approaches that detect and mitigate malicious behavior after the fact, proactive security emphasizes protecting the authenticity, integrity, confidentiality, and privacy of communication through preventive cryptographic and architectural measures. This approach is particularly vital in V2X environments, which are characterized by highly dynamic topologies, stringent real-time requirements, and safety-critical functions.

The deployment of Public Key Infrastructure (PKI)-based solutions is fundamental to proactive V2X security. PKI facilitates message authentication, integrity verification, and non-repudiation using digital signatures and certificates. Standardization bodies such as IEEE and ETSI have established PKI-based security architectures, including IEEE 1609.2 and ETSI TS 103 097, which define secure message formats and certificate management protocols for vehicular communications. These mechanisms restrict V2X communication to legitimate entities, thereby mitigating impersonation and basic spoofing attacks.

To address privacy concerns, proactive security frameworks employ pseudonymous certificates, enabling vehicles to periodically update their identifiers while preserving authentication. This strategy reduces risks associated with location tracking and profiling by preventing the persistent linking of transmitted messages to actual vehicle identities. The survey highlights that

pseudonym management is both essential and challenging, as frequent certificate changes elevate signaling overhead and complicate revocation processes.

Another critical category of proactive mechanisms addresses secure key management and certificate revocation. Compromised or misbehaving vehicles pose significant threats to V2X ecosystems, necessitating efficient revocation strategies to promptly exclude them. The literature discusses Certificate Revocation Lists (CRLs) and alternative methods, such as compressed CRLs and regional revocation schemes, that aim to balance security effectiveness with communication efficiency. Nevertheless, scalability remains a major challenge, particularly in high-density traffic environments.

Secure hardware components, such as Hardware Security Modules (HSMs), are also identified as integral to proactive security. HSMs offer tamper-resistant environments for cryptographic operations and secure key storage, thereby substantially reducing the risk of key extraction and physical attacks. These components are commonly incorporated in both academic proposals and standard frameworks for V2X security architecture.

Despite their effectiveness, proactive security mechanisms have inherent limitations. Cryptographic operations incur computational and communication overhead that can conflict with the low-latency requirements of safety-critical V2X applications. Furthermore, proactive approaches are generally ineffective against insider attacks and compromised yet authenticated nodes, as they rely on the presumed trustworthiness of entities with valid credentials. The authors contend that while proactive security is essential, it must be supplemented by reactive and trust-based mechanisms.

Proactive security mechanisms form the foundational layer of V2X cybersecurity, establishing trust, authenticity, and privacy through standardized cryptographic solutions. [5] Nonetheless, persistent challenges in scalability, latency, revocation efficiency, and insider threats necessitate integrating proactive measures with adaptive, intelligence-driven security solutions, as explored in subsequent sections of the survey.

VI. REACTIVE SECURITY MECHANISMS IN V2X COMMUNICATION

Reactive security mechanisms in Vehicle-to-Everything (V2X) communication are intended to detect, identify, and mitigate malicious behavior after an attack has commenced. [5] In contrast to proactive approaches that prevent unauthorized participation through cryptographic safeguards, reactive security targets originate from authenticated or compromised entities, such as insider nodes and misbehaving vehicles. This function is essential in V2X environments, where high mobility, openness, and decentralized operation render preventive security alone inadequate.

Misbehavior detection is a primary category of reactive security solutions that focuses on identifying abnormal or malicious actions by analyzing transmitted messages and

vehicle behavior. The survey examines various mechanisms for detecting misbehavior, including plausibility checks, consistency verification, and context-aware analysis. For instance, these methods detect physically impossible positions, unrealistic speeds, or inconsistent trajectories among neighboring vehicles. Such approaches assume that legitimate vehicle behavior adheres to predictable physical and spatiotemporal constraints.

Reactive security mechanisms are generally categorized into local and cooperative detection strategies. Local mechanisms operate independently within individual vehicles, providing rapid response and minimal communication overhead, though they may suffer limited visibility and higher false-positive rates. In contrast, cooperative mechanisms utilize information sharing among multiple vehicles or infrastructure nodes to enhance detection accuracy and robustness. However, cooperative schemes present challenges related to trust management, scalability, and increased communication overhead.

Trust and reputation management is a significant aspect of reactive security discussed in the survey. Trust-based frameworks dynamically assign trust scores to vehicles according to their observed behavior over time. Vehicles that consistently transmit valid and plausible information are deemed trustworthy, whereas misbehaving entities experience a degradation of trust and eventual isolation. These mechanisms facilitate adaptive responses to evolving attacks but must be carefully designed to prevent manipulation, collusion, and Sybil attacks.

The survey highlights the growing importance of machine learning and data-driven techniques in reactive V2X security. Supervised, unsupervised, and semi-supervised learning models are utilized to classify normal and malicious communication patterns, detect anomalies, and identify emerging threats. These approaches show considerable potential for addressing complex and previously unknown attacks. However, the survey also notes that learning-based solutions introduce new vulnerabilities, including adversarial machine learning and data poisoning, which must be addressed in system design.

Despite their effectiveness, reactive security mechanisms exhibit significant limitations. Detection latency can permit short-lived attacks to affect safety-critical services before mitigation is possible. Furthermore, the absence of standardized datasets and evaluation methodologies complicates objective performance comparisons across detection schemes. Excessive false alarms may also undermine system trust and usability, particularly in dense traffic environments.

In summary, reactive security mechanisms are essential complements to proactive defenses in V2X communication. By facilitating the detection and mitigation of insider attacks, compromised nodes, and unforeseen threats, these mechanisms strengthen the resilience of V2X ecosystems. However, the survey emphasizes that integrating reactive mechanisms with proactive security and trust frameworks is necessary to

achieve comprehensive, robust cybersecurity in intelligent transportation systems.

VII. THE ROLE OF ARTIFICIAL INTELLIGENCE IN V2X SECURITY

Artificial Intelligence (AI) has become a key enabler of improved cybersecurity in Vehicle-to-Everything (V2X) communication systems, especially for addressing complex, dynamic, and previously unknown attack scenarios. While traditional rule-based and cryptographic security mechanisms remain essential, they are often inadequate for managing the scale, mobility, and heterogeneity of V2X environments. [5] Consequently, recent literature increasingly investigates machine learning (ML) and data-driven approaches to supplement both proactive and reactive security mechanisms.

A central application of AI in V2X security is the detection of anomalies and misbehavior. Machine learning models are trained to recognize normal communication and mobility patterns using historical or real-time data, enabling the identification of deviations that may signal malicious activity. Supervised learning techniques, such as support vector machines, decision trees, and neural networks, are effective when labeled datasets are available. Conversely, unsupervised and semi-supervised methods, including clustering and autoencoders, are used to detect novel or previously unknown attacks that require labeled data. These methods are particularly valuable in V2X environments, where attack patterns can change rapidly.

AI-based security mechanisms are also implemented in trust and reputation management systems. Learning-based trust models analyze vehicle behavior over time to dynamically update trust scores and identify persistently malicious or unreliable nodes. Compared to static rule-based frameworks, AI-driven approaches provide greater adaptability and scalability in dynamic traffic conditions. However, the survey notes that these systems are sensitive to data quality and susceptible to manipulation through coordinated or collusion attacks.

Another significant research direction focuses on intelligent intrusion detection systems (IDS) designed for V2X communication. These systems combine data from various sources, such as onboard sensors, network traffic, and contextual information, to achieve more accurate and timely detection. Deep learning models, including convolutional and recurrent neural networks, show considerable promise in capturing the complex spatiotemporal dependencies present in vehicular environments. However, their computational and training demands pose challenges for deployment on resource-constrained vehicular nodes.

Despite their benefits, AI-driven security solutions introduce new threat vectors. The survey identifies vulnerabilities unique to machine learning, such as adversarial examples, data poisoning, and model manipulation. Attackers can inject malicious data during training or operation to reduce detection accuracy or bias trust assessments. These risks raise significant concerns about the reliability and robustness of AI-based V2X

security mechanisms, particularly in safety-critical applications.

Furthermore, the absence of standardized datasets, benchmarks, and evaluation frameworks remains a major barrier to the adoption of AI solutions in V2X security. Many studies rely on simulation-based datasets or simplified assumptions, complicating cross-comparison and limiting real-world validation. The authors emphasize the need for realistic, large-scale datasets and reproducible evaluation methodologies to advance research in this field.

In summary, artificial intelligence offers significant potential for enhancing cybersecurity in V2X communication by enabling adaptive, data-driven detection and decision-making. However, effective integration requires careful attention to robustness, explainability, computational efficiency, and protection against AI-specific attacks. The survey concludes that future V2X security architectures should integrate AI-based mechanisms with traditional proactive and reactive defenses to achieve resilient and trustworthy intelligent transportation systems.

VIII. OUTSTANDING CHALLENGES AND DIRECTIONS FOR FUTURE RESEARCH

Although significant advancements have been made in securing Vehicle-to-Everything (V2X) communications, several unresolved challenges hinder the deployment of fully resilient intelligent transportation systems. A primary concern is the pronounced interdependence between cybersecurity and functional safety. In contrast to traditional networks, successful cyberattacks on V2X systems can directly threaten human safety. However, most current security solutions are not adequately integrated with safety certification and system-level assurance frameworks. Consequently, future research should prioritize integrated security and safety co-design methodologies.

Scalability and latency constraints constitute another significant challenge. Cryptographic authentication, certificate management, and revocation mechanisms introduce processing and communication overhead, which can conflict with stringent real-time requirements, especially in dense traffic environments. As V2X deployments increase, the development of lightweight and latency-aware security mechanisms is essential.

Trust and reputation management in highly dynamic and decentralized environments remains an unresolved issue. While trust-based schemes offer adaptability, they are susceptible to collusion, Sybil attacks, and manipulation of trust metrics. Developing robust, context-aware trust models that function reliably under partial observability and adversarial conditions represents a critical research direction.

The growing integration of artificial intelligence amplifies both opportunities and risks within V2X systems. Although AI-based mechanisms enhance adaptability and detection accuracy, they also introduce vulnerabilities, including adversarial machine learning and data poisoning. Ensuring the robustness, transparency, and verifiability of

AI models is therefore essential for safety-critical V2X applications.

The absence of standardized datasets, benchmarks, and evaluation methodologies, combined with interoperability and regulatory challenges, significantly impedes real-world adoption. Future research should advance holistic, scalable, and adaptive security architectures that integrate proactive, reactive, and AI-driven solutions to enable trustworthy and resilient V2X-enabled intelligent transportation systems.

IX. CONCLUSION

Intelligent Transportation Systems (ITS) increasingly depend on Vehicle-to-Everything (V2X) communication and distributed cyber-physical architectures to improve safety, efficiency, and automation. [28] However, this increased connectivity substantially enlarges the attack surface, underscoring the need for cybersecurity to ensure the reliable operation of modern transportation systems. This paper examines cybersecurity threats in ITS using a structured, multi-dimensional perspective, emphasizing their complexity and potential cyber-physical consequences.

A comprehensive classification of threats is presented, considering threat actors, attack vectors, targeted assets, violated security properties, and resulting impacts. The analysis demonstrates that cybersecurity incidents in ITS frequently extend beyond the digital domain, directly impacting system availability, operational reliability, and road safety. This characteristic distinguishes ITS from traditional information systems and underscores the need for integrated, safety-aware security strategies.

The paper further reviews proactive and reactive security mechanisms for V2X communication. Proactive approaches, such as PKI-based authentication and privacy-preserving mechanisms, establish a necessary baseline of trust but encounter limitations in scalability, latency, and the threat of insider attacks. Reactive mechanisms, including misbehavior detection and trust-based frameworks, complement these defenses by enabling the identification of compromised or malicious nodes during operation, although challenges remain in detection accuracy and timely response.

Artificial intelligence is identified as a powerful enabler of adaptive, data-driven security, capable of addressing complex, evolving attack scenarios. However, AI-based solutions also introduce new vulnerabilities, reinforcing the need for robust, explainable, and verifiable models in safety-critical environments.

In conclusion, achieving resilient and trustworthy intelligent transportation systems requires a holistic cybersecurity approach that integrates proactive, reactive, and AI-driven mechanisms within a unified framework. The solution pathways discussed in this work are intended to support scalable, adaptive, and safety-aware security architectures, thereby contributing to the secure evolution of next-generation ITS.

ACKNOWLEDGMENT

The authors thank their affiliated institutions for their support of this research. They also appreciate the helpful discussions and technical insights that shaped this work.

REFERENCES

- [1] S. Joshi, A. Baviskar and S. Rajmane, "A review of cybersecurity in smart cities and intelligent transport systems," *Discover Internet of Things*, vol. 6, p. 41, 2026.
- [2] Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z., "Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions," in *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*, Kyiv, Ukraine, February 28, 2025 (online).
- [3] E. Dritsas and M. Trigka, "A Survey on Cybersecurity in IoT," *Future Internet*, vol. 17, 2025.
- [4] U. Tariq, I. Ahmed, A. K. Bashir and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review.," *Sensors (Basel, Switzerland)*, vol. 23, no. 8, April 2023.
- [5] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso and J. Alonso-Zarate, "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 325-391, 2023.
- [6] K. Herman Muraro Gualarte, J. Paulo Javidi da Costa, J. A. R. Vargas, A. Santos da Silva, G. Almeida Santos, Y. Wang, C. Alfons Müller, C. Lipps, R. Timóteo de Sousa, W. de Brito Vidal Filho, P. Slusallek and H. Dieter Schotten, "Integrating Cybersecurity in V2X: A Review of Simulation Environments," *IEEE Access*, vol. 12, pp. 177946-177985, 2024.
- [7] R. K. Agrawal, *AI-Driven Secure Vehicular Networks: Intelligent Threat Detection and Trust-Aware Defense for V2X Systems*, IEEE Dataport, 2026.
- [8] F. C. Ogenyi, C. N. Ugwu and O. P.-C. Ugwu, "Securing the future: AI-driven cybersecurity in the age of autonomous IoT," *Frontiers in the Internet of Things*, Vols. Volume 4 - 2025, 2025.
- [9] O. Grant, "Smart ITS: AI, V2X, Sensors, Security," *Global Journal of Technology and Optimization*, vol. 16, no. 4, 2025.
- [10] V. Sokolov, F. Kipchuk, P. Skladannyi, O. Zhylytsov and D. Ageyev, "Method for Increasing the Various Sources Data Consistency for IoT Sensors," in *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 2022.
- [11] Dudykevych, V. and Mykytyn, G. and Stosyk, T. and Skladannyi, Pavlo, "Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society," *Cybersecurity Providing in Information and Telecommunication Systems 2024*, vol. 3654, pp. pp. 449-457, 2024.
- [12] V. Sokolov, P. Skladannyi and N. Mazur, "Wi-Fi Repeater Influence on Wireless Access," in *2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, 2023.
- [13] 3GPP, "Service requirements for enhanced V2X scenarios (Release 17)," *Tech. Rep. TS 22.186 v17.0.0*, 2022.
- [14] B. Brecht, D. Theriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, pp. 3850-3871, December 2018.
- [15] A. Alnasser, H. Sun and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52-67, 2019.
- [16] M. Hasan, S. Mohan, T. Shimizu and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, pp. 693-713, December 2020.
- [17] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33-50, 2017.
- [18] M. Villarreal-Vasquez, B. K. Bhargava and P. Angin, "Adaptable Safety and Security in V2X Systems," *2017 IEEE International Congress on Internet of Things (ICIOT)*, pp. 17-22, 2017.
- [19] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55-82, 2018.
- [20] ETSI, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2," *Tech. Rep. TS 102 940 V2.1.1*, 2021.
- [21] D. Manivannan, S. S. Moni and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETWORKS (VANETs)," *Veh. Commun.*, vol. 25, p. 100247, 2020.
- [22] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
- [23] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*, USA, 2011.
- [24] I. Ivanov, C. Maple, T. Watson and S. Lee, "Cyber Security Standards and Issues in V2X Communications for Internet of Vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, p. 46.
- [25] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, p. 39-68, January 2007.
- [26] R. Lu, L. Zhang, J. Ni and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE*, vol. 108, pp. 373-389, February 2020.
- [27] S. Sharma, A. Kaul, S. Ahmed and S. Sharma, "A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions," *International Journal of Communication Systems*, vol. 34, p. e4905, 2021.
- [28] D., Dimitrov, *Intelligent Transportation Management: Current Issues and Solutions*, LAP LAMBERT Academic Publishing, pp. 284, 2026.

Evaluation of the Performance of Classification Algorithms in the QGIS System

Peter Grabusts

Engineering Centre

Rezekne Academy of Riga Technical University

Rezekne, Latvia

peteris.grabusts@rtu.lv

Jurijs Musatovs

Engineering Centre

Rezekne Academy of Riga Technical University

Rezekne, Latvia

jurijs.musatovs@rtu.lv

Abstract—The use of lake reeds as a source of green energy is becoming increasingly significant. Accurate estimation of reed-covered areas is essential, as it enables forecasting of potential biomass yields and supports carbon footprint calculations. However, in Latvia, there is currently a lack of comprehensive research on the availability and spatial distribution of reeds. The main objective of this research is to develop a method for modeling the distribution of lake reeds in order to predict their future availability. The research focuses on satellite imagery of lakes, with spatial analysis and modeling performed using QGIS. A critical stage in the methodology is classification, which allows reeds to be distinguished from surrounding land cover types and enables estimation of their extent within lake environments. For this purpose, several semi-automatic classification algorithms were applied, including Minimum Distance and Random Forest. The performance of these algorithms was evaluated experimentally, and the most suitable approach was selected based on its agreement with available historical data.

Keywords—reeds, classification algorithms, modeling, satellite data, QGIS

I. INTRODUCTION

Alongside economic development, demand for renewable energy is increasing due to its sustainability and lower environmental impact compared to fossil fuels. Among renewable energy sources, biomass remains one of the most widely utilized. Current trends emphasize the use of non-traditional biomass sources, including cultivated energy crops, wood residues, and aquatic vegetation such as reeds.

With rising fossil fuel prices and growing concern over environmental pollution, interest in locally available biomass resources for energy production is steadily increasing. As a result, the rational and efficient use of reed resources has become an important research topic.

Reed (*Phragmites australis*) [1] is a widespread plant species in Latvia that has traditionally been regarded as a nuisance due to its rapid expansion in water bodies. Reed-

covered areas continue to increase, and mowing is often carried out to control overgrowth in lakes and other aquatic environments. At the same time, these ecosystems contain substantial amounts of reed biomass, which remains an underutilized renewable energy resource. Despite its high availability and potential, reed is currently used only to a limited extent in Latvia, primarily in construction, such as for roofing materials.

Existing literature reports a wide range of values for reed biomass yield. For instance, the amount of biomass obtained from winter harvesting varies significantly, ranging from 3 to 30 t/ha [2]. This variability highlights the need for more precise and location-specific assessments.

To evaluate the potential use of reeds as a biomass resource, it is essential to accurately determine reed-covered areas within individual lakes and to monitor their changes over time. Such analysis enables the prediction of trends in reed expansion or decline. In this context, Geographic Information Systems (GIS), such as QGIS, provide powerful tools for analyzing satellite imagery across different time periods, calculating reed area within defined reference intervals, and modeling future spatial dynamics [3] – [6].

The paper [7] examines a significant ecological monitoring problem – changes in the degradation and distribution of aquatic reeds in European lakes. Given that traditional monitoring methods are expensive and time-consuming, the study shows that Green Li-DAR technology can significantly improve the efficiency and accuracy of monitoring. This is especially important for smaller lakes, where the resolution of satellite images is insufficient.

The paper [8] analyses the biomass potential of common reed in the wetlands of the Syr Darya Delta region of Kazakhstan using remote sensing data and Random Forest machine learning models. The authors combine field measurements with high-resolution Sentinel satellite images to create a spatially detailed map of reed biomass and estimate the resource volume in arid climate conditions

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.196>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

near the former Aral Sea. The main advantage of the study is the methodological approach - the integration of precise field data with satellite images and improved regression models allows for reliable biomass estimates. The performance indicators of the models are particularly convincing, indicating high forecast accuracy. The authors find that the largest biomass is concentrated along river branches and lake shores, where water availability is stable.

This research aimed to develop a methodology for identifying reed-covered areas in lakes. Satellite imagery was obtained from the Copernicus Sentinel database and processed using the QGIS environment. Known land cover classes – such as water, forest, soil, grass, and reeds – were identified and used for classification. The accuracy of the results depends heavily on how precisely these classes are defined.

To determine the most suitable approach, several classification algorithms were tested, including Minimum Distance, Multilayer Perceptron, Random Forest, and Support Vector Machine. A significant amount of time was devoted to selecting appropriate satellite images, as cloud cover is frequent in Latvia even during summer, making image quality a critical factor.

The results demonstrated that the estimated proportion of reed-covered areas in Lake Rāzna is consistent with findings reported in other scientific studies, indicating that the proposed methodology has strong potential for further development. This work builds upon previous research presented in article [9].

II. MATERIALS AND METHODS

A. Research Object

The object of this research is Lake Rāzna (see Fig. 1), which is the second-largest lake in Latvia [10]. The lake's key characteristics are summarized in Table 1.



Fig. 1. Lake Rāzna.

TABLE 1 LAKE CHARACTERISTIC

Characteristic	Parameter
Coordinates	56°19'N 27°27'E
Area of water surface	5,756.4 hectare
Mean depth	7.0 metre(s)
Maximum depth	17.0 metre(s)
volume	405.000 million solid metres
Length of lakeshore line	43.5 kilometre

Maximum length	12.10 kilometre
Maximum width	7.00 kilometre
Average altitude (above sea level)	163.40 metre(s)
Maximum altitude (above sea level)	163.50 metre(s)

Sentinel-2 images of Lake Rāzna look very impressive, because it is a big water square and the complex shoreline is very visible even with 10 m resolution:

- Lake appears dark blue or almost black because deep water absorbs light.
- Coastal in the shallows, water is brighter, sometimes with a green pasture tone.
- Coastline is very twisted, with many folds and peninsulas.
- Surrounding fields and forests form a contrasting mosaic.

B. Satellite Data and QGIS

The study utilised data from the Copernicus Programme Sentinel satellites, one of the most valuable open-access Earth observation resources worldwide. The Sentinel system consists of a series of satellites developed specifically for the Copernicus programme [11], [12].

Among these, Sentinel-2 plays a particularly important role in land monitoring. Its primary application areas include agriculture, vegetation analysis, land cover classification, and fire monitoring. Sentinel-2 provides high spatial resolution imagery (10–20 m) and frequent revisit times (approximately every 5 days), making it one of the most powerful tools currently available for open-access environmental mapping.

Satellite data from Copernicus support a wide range of users, including service providers, governmental institutions, and research organisations, enabling efficient acquisition and analysis of environmental information. These data and derived information services are freely available to users, significantly enhancing accessibility.

In this research, Sentinel-2 satellite imagery was used for the detection of lake reed areas, and the data were subsequently processed using the QGIS environment [13].

QGIS is a free and open-source Geographic Information System (GIS) that enables users to view, edit, and analyse spatial data, create maps, process satellite imagery, and perform spatial analysis and modelling. It is a powerful tool for cartographic production and geospatial data processing, offering extensive functionality through a wide range of plugins. QGIS supports both raster and vector data formats and integrates numerous open-source libraries to ensure compatibility with diverse geospatial datasets.

QGIS is one of the most widely used GIS platforms globally due to its lack of licensing costs, cross-platform compatibility, support for multiple data formats, and a large ecosystem of community-developed plugins.

Among these plugins, the Semi-Automatic Classification Plugin (SCP) was used in this study. SCP is

one of the most powerful and widely used tools within QGIS for processing and analysing Sentinel-2 satellite imagery. In this study, it was applied for image classification to distinguish reed-covered areas from other land cover classes.

C. Classification Algorithms

To detect reeds in lakes using GIS, it is necessary to combine several methods. First, satellite data is used to identify various objects in the surrounding field. Second, these objects are classified to distinguish reeds.

We chose the following classification of objects and their designations (see Fig.2).



Fig.2. Classification of objects (legends).

The following discusses four popular classification algorithms that will be used in reed recognition: Minimum Distance, Multilayer Perceptron, Random Forest, and Support Vector Machine.

Minimum Distance.

Minimum Distance Estimation (MDE) [14] is a statistical parameter estimation approach that seeks model parameters that minimize the "distance" between the theoretical (model) distribution and the empirical (observed data) distribution.

The essence of the algorithm is as follows: for a given point x , the distances to all candidates (e.g., classes or nodes) are computed, and the one with the smallest distance is selected.

The most commonly used distance measure is the Euclidean distance:

$$d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}, \quad (1)$$

where x and y are vectors in n -dimensional space, and x_i, y_i - their components.

Algorithm steps:

1. Input:
 - Dataset (points or class representatives).
 - New point x that needs to be classified or analyzed.
2. Distance calculation:

- Calculates the distance between x and each element of the data set.

3. Finding the minimum:

- Finds the element with the smallest distance.

4. Result:

- In case of classification: assigns a class to the closest element.
- In case of graphs: chooses the shortest path.

Advantages: simple implementation, intuitive, and no complex training required.

Disadvantages: slow for large data sets, sensitive to noise and scale, and depends on the chosen distance measure.

Multilayer Perceptron.

A multilayer perceptron (MLP) [15] is an artificial neural network widely used in machine learning and deep learning tasks. It consists of multiple layers of neurons and is widely used in classification and regression tasks.

MLP consists of:

Input layer – receives data;

Hidden layers – performs calculations and feature transformation;

Output layer – produces a result.

Each neuron calculates a weighted sum and applies an activation function:

$$y = f\left(\sum_i w_i x_i + b\right), \quad (2)$$

where w_i – weights, b – bias, f – activation function (relu, sigmoid, or others).

Algorithm steps:

1. Initialization:

Randomly initialize weights and biases.

2. Forward propagation:

Data is fed through the network from the input to the output. Each layer computes its own output.

3. Error calculation:

Compares the predicted result with the true value.

Uses a loss function (e.g., MSE or cross-entropy).

4. Backpropagation:

Computes the error gradients with respect to the weights, based on gradient descent.

5. Weight update:

Weights are adjusted to reduce the error.

6. Iteration:

The process is repeated for several epochs until the model converges.

Advantages: able to model nonlinear relationships, universal approximator, flexible architecture.

Disadvantages: requires a lot of data, can overfit, difficult to interpret ("black box"), sensitive to hyperparameters.

Random Forest.

Random Forest [16] is an ensemble machine learning method that relies on combining many decision trees to obtain a more accurate and stable prediction.

The idea of Random Forest is based on the fact that several "weak" models (decision trees) can together form a strong model.

Each tree is trained on a randomly selected subset of data. A random subset of features is used in each splitting step. The final result in classification is obtained by voting (majority vote).

Algorithm steps:

1. Data sampling (Bootstrap):

Randomly select subsets from the original data set (with repetition).

2. Tree building:

For each tree, a random subset of features is selected at each node, and the best distribution is found according to a criterion (e.g., Gini index).

3. Model merging: in classification - voting

4. Prediction for new data: each tree gives a result, and the final result is the combined result.

Advantages: high accuracy, reduces overtraining compared to a single tree, and works well with large and complex data.

Disadvantages: more difficult to interpret than a single decision tree, requires more computing resources, and is slower in prediction.

Support Vector Machine.

Support Vector Machine (SVM) [17] is a supervised machine learning algorithm used for classification and regression. Its basic idea is to find a boundary (hyperplane) that best separates data into different classes.

SVM attempts to find a hyperplane that separates the data into two classes and maximizes the margin to the nearest points:

$$w^T x + b = 0 \quad (3)$$

Support vectors are the points closest to the boundary; they determine the position of the hyperplane, and only these points affect the model.

The SVM solves the equation:

$$\min_{w,b} \frac{1}{2} \|w\|^2 \quad (4)$$

with the condition

$$y_i(w^T x_i + b) \geq 1 \quad (5)$$

This means that the weight norm is minimized and correct classification is ensured.

If the data is not linearly separable, SVM uses kernel functions to transform the data into a higher dimension. The most popular kernels are linear, polynomial, and RBF (Gaussian).

Algorithm steps:

1. Choose a kernel function.

2. Formulate the optimization problem.

3. Solve the quadratic programming problem.

4. Identify support vectors.

5. Construct a classification function.

Advantages: efficient on high-dimensional data, good with small amounts of data, and strong theoretical basis.

Disadvantages: slow for large data sets, sensitive to parameter selection (kernel), and more difficult to interpret.

III. RESULTS AND DISCUSSION

In the authors' previous work [9], a study was conducted with satellite data of Lake Rāzna for different years to classify objects with the Random Forest algorithm using QGIS and separate reeds from other objects around the lake.

The research methodology is based on the following sequence of actions:

- a suitable lake map with 5% cloudiness is found using Copernicus;
- suitable objects are identified for classification purposes in the QGIS environment (according to the legends in Figure 2);
- a classification algorithm is selected from SCP options;
- classification is performed, and the obtained results are analyzed.

The classification results are shown in Figure 3 and Table 2.

TABLE 2 CLASSIFICATION RESULTS (YEAR 2024)

Raster value	Pixel Sum	Percent age %	Area (m ²)	Area (hectare)
1-Water	529140	6.03	52914000	5291.40
2-Reed	266918	3.04	26691800	2669.18
3-Wood	4599805	52.39	459980500	45998.05
4-Soil	412493	4.70	41249300	4124.93
5-Grass	2972380	33.85	297238000	29723.80

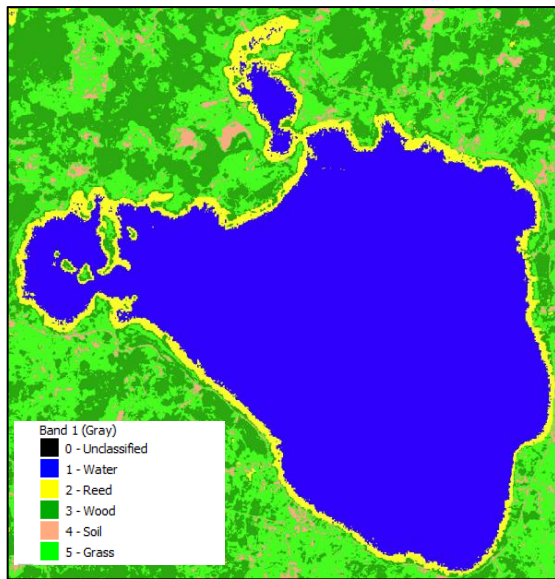


Fig.3. Reeds (yellow) in Lake Rāzna (year 2024).

From now on, we will use only the percentage of reeds in the water surface area of Lake Rāzna in 2024 to evaluate the performance of various classification algorithms.

We will have the opportunity to compare the experimental results with data from [2], which reported that in 2008 the area of reeds constituted approximately 4 percent of the water surface area.

Five experiments were performed for each algorithm. Of course, the initial settings and parameters in classification algorithms are different, but our task is to determine the suitability of the algorithms for classifying reeds.

Minimum Distance.

For the Minimum Distance algorithm in the SCP, the threshold value represents a minimum probability percentage (0–100).

Experiment 1: Very Strict: Only pixels with very high probability (95%+ confidence) are classified. Best for homogeneous areas where you need high confidence, but will leave many pixels unclassified.

Experiment 2: Strict: A common starting point for high-quality results. Filters out most ambiguous pixels while retaining well-defined features.

Experiment 3: Moderate: A balanced threshold. Allows more pixels to be classified while still rejecting many uncertain ones. Useful for heterogeneous landscapes.

Experiment 4: Relaxed: Includes a wider range of probabilities. Suitable for initial exploratory runs or when you want to minimize unclassified areas at the cost of potential noise.

Experiment 5: No Threshold: Classifies every pixel. All pixels are assigned to the class with the highest probability, regardless of how low that probability is. This is the default behavior when the threshold option is unchecked.

The results for the Minimum Distance algorithm are shown in Table 3.

TABLE 3 MINIMUM DISTANCE RESULTS

N	Probability percentage	Reeds (%)
1	95	3.88
2	90	4.09
3	80	4.35
4	70	4.48
5	0	3.45

Score range: 3.45 - 4.48. Average value: 4.05.

Multilayer Perceptron.

Unlike the Minimum Distance algorithm, the MLP is a neural network with many tunable parameters that control its architecture and learning behaviour.

Experiment 1: Baseline (Default Configuration). One hidden layer with 100 neurons, activation – relu, learning rate – 0.001.

Experiment 2: Simple Architecture (Reduced Complexity). Uses a much smaller network with only 10 neurons in a single hidden layer. This creates a simpler model that is less likely to overfit on small training datasets. Activation – relu, learning rate – 0.001.

Experiment 3: Deep Architecture (Increased Complexity). Uses three hidden layers with 50 neurons each. This creates a deeper network capable of learning more complex patterns, at the risk of overfitting. Activation – relu, learning rate – 0.001.

Experiment 4: Strong Regularization (Overfitting Prevention). Increases the alpha regularization parameter from 0.0001 to 0.01. A higher alpha adds more penalty for large weights, producing a simpler, more generalized model. Activation – relu, learning rate – 0.001.

Experiment 5: Slow Learning with SGD. Uses the SGD (Stochastic Gradient Descent) solver, with a higher learning rate (0.01) and tanh activation function. This configuration learns more slowly and may generalize differently.

The results for the MLP algorithm are shown in Table 4.

TABLE 4 MLP RESULTS

N	Model	Reeds (%)
1	Baseline	7.54
2	Simple architecture	4.84
3	Deep architecture	5.87
4	Strong regularization	5.52
5	Slow learning	-

Score range: 4.84 - 7.54. Average value: 5.94.

Random Forest.

For the Random Forest algorithm in the SCP, the main parameter is the number of trees.

Experiment 1: Baseline (Fast Preview). This configuration prioritizes speed and is ideal for initial previews before committing to a full classification.

Experiment 2: Standard Forest. This configuration matches parameters used in published remote sensing studies with SCP. A study on mangrove forest mapping achieved 99.12% accuracy using these settings.

Experiment 3: Large Forest. The SCP documentation explicitly recommends that "Number of trees should be at least 500 for good results" in production classifications.

Experiment 4: Very Large Forest (Maximum Accuracy). For final production maps, where accuracy is critical and processing time is not a limiting factor. The typical range for estimators is 100 to 1000.

Experiment 5: Conservative Splitting (Overfitting Prevention). Requires more samples per internal node – min samples to fit – 5. This is useful when you have a small training dataset and want to avoid overly complex trees that memorize noise rather than generalizing patterns.

The results for the Random Forest algorithm are shown in Table 5.

TABLE 5 RANDOM FORESTS RESULTS

N	Number of trees	Reeds (%)
1	10	5.80
2	100	4.67
3	500	5.06
4	1000	4.63
5	100	5.15

Score range: 4.63 - 5.80. Average value: 5.06.

Support Vector Machine.

For the SVM algorithm in the SCP, the key adjustable parameters are Kernel type, Gamma, and Cost (C). Gamma controls the influence of a single training sample, while Cost (C) controls the trade-off between minimizing error on the training data and maintaining a simple decision boundary. The kernel type traditionally is Radial Basis Function.

Experiment 1: Baseline (Default Configuration). This experiment uses the standard defaults for SVM classification. It serves as a control group for comparing other variations.

Experiment 2: Low Gamma (Smooth Decision Boundary). This experiment uses a smaller Gamma value, which means each training sample has a wider influence radius. The resulting decision boundary will be smoother and more generalized.

Experiment 3: High Gamma (Detailed Decision Boundary). This experiment uses a larger Gamma value, which means each training sample has a narrow influence radius. The decision boundary will be more detailed and can capture complex patterns. A high gamma creates a more detailed, potentially "wiggly" decision boundary. This can capture fine spatial patterns, but risks overfitting if your training data has outliers or noise

Experiment 4: Low Regularization (Higher Penalty for Errors). This experiment increases the Cost parameter. A higher C value tells the algorithm to work harder to classify every training sample correctly, even if that means creating a more complex boundary. With higher C, the classifier tries harder to fit the training data exactly. This can improve accuracy but increases the risk of overfitting to noise in data samples.

Experiment 5: High Regularization (Softer Penalty for Errors). This experiment decreases the Cost parameter. A lower C value allows more training samples to be misclassified if it leads to a simpler, more generalized decision boundary. Lower C creates a softer, more generalized boundary that may ignore some training samples.

The results for the SVM algorithm are shown in Table 6.

TABLE 6 SVM RESULTS

N	Gamma	Cost	Reeds (%)
1	0.1	1	4.71
2	0.01	1	5.36
3	1	1	6.70
4	0.1	10	4.73
5	0.1	0.1	4.77

Score range: 4.71 - 6.70. Average value: 5.25.

The model trained with the classification data from Lake Rāzna produced the following results: Training Accuracy: 98.39%, Validation Accuracy: 98.74%.

The most important limiting factors of the research are the following:

- Geographic limitations.

The research focuses on Latvian lake ecosystems, which may limit the applicability of results to regions with different climatic, hydrological, or ecological characteristics. Limitations related to satellite data and resolution.

- Classification model limitations.

The neural network model trained using SCP was validated on a limited number of lake areas, which may reduce generalizability to other lakes with different hydrological or ecological conditions. Potential misclassification of vegetation may influence the estimated reed-covered area and, consequently, biomass calculations.

IV. CONCLUSIONS

This research evaluated the effectiveness of several classification algorithms for identifying reed-covered areas in Lake Rāzna using Sentinel-2 satellite imagery and the QGIS environment. Four algorithms were experimentally tested — the Minimum Distance algorithm, Multilayer Perceptron, Random Forest, and Support Vector Machine — each through five experiments with different parameter settings.

The Minimum Distance algorithm demonstrated the closest agreement with available historical data: the average calculated reed coverage was 4.05%, which closely matches the estimate reported in a 2008 study [2]

(approximately 4% of the lake surface area). The Random Forest algorithm produced an average value of 5.06%, while the Support Vector Machine yielded 5.25%. The Multilayer Perceptron produced the highest average value (5.94%) and also showed the greatest variability between experiments, indicating higher sensitivity to parameter selection.

Overall, the research confirms that the developed methodology — based on Sentinel-2 satellite image processing in the QGIS environment and established classification techniques — is suitable for determining reed distribution and monitoring their spatial changes over time. The Minimum Distance and Random Forest algorithms appear particularly promising: the former provides a simple and reliable baseline estimate, while the latter offers greater suitability for more complex landscape structures and heterogeneous environments.

Future research will focus on improving the assessment of reed biomass potential in lakes and evaluating the carbon footprint associated with industrial reed processing.

V. ACKNOWLEDGMENTS

This research was funded by grant number RTU-PA-2024/1-0077, “Towards a sustainable bioeconomy: assessing reed biomass potential and applications (ReedREvolution)”.

REFERENCES

- [1] “Plant family,” [Online] Available: <https://www.britannica.com/plant/Poaceae> [Accessed: Feb. 20, 2026].
- [2] E.Čubars and G. Noviks, Influence of Different Factors on Productivity of Reed Growths, Environment. Technology. Resources, Proceedings of the 9th International Scientific and Practical Conference, Volume 1, Rezekne, Latvia, 2013. <https://doi.org/10.17770/etr2013vol1.801>
- [3] E.Tiškus, D.Vaičiūtė, M.Bučas, and J. Gintauskas, "Evaluation of common reed (*Phragmites australis*) bed changes in the context of management using earth observation and automatic threshold," European Journal of Remote Sensing, 2022. <https://doi.org/10.1080/22797254.2022.2161070>
- [4] L. Sciuto, F. Licciardello, A.C. Barbera, and G. Cirelli, "A GIS - based multicriteria decision analysis to reduce riparian vegetation hydrogeological risk and to quantify harvested biomass (Giant reed) for energetic retrieval," Ecological Indicators, Volume 144, November 2022, <https://doi.org/10.1016/j.ecolind.2022.109548>
- [5] S. Baier, N.C. Meneses, J. Geist, and T. Schneider, "Assessment of Aquatic Reed Stands from Airborne Photogrammetric 3K Data," Remote Sens. 14(2), 337, 2022, <https://doi.org/10.3390/rs14020337>
- [6] H. Runkui and L. Yuqin, "Application of remote sensing technique to the investigation on reed resources of Bosten Lake," Chinese Geographical Science, Volume 2, pages 266–276, 1992, <https://doi.org/10.1007/BF02664604>
- [7] S. Baier, N.C. Meneses, J. Geist and T. Schneider, "Assessment of Aquatic Reed Stands from Airborne Photogrammetric 3K Data. Remote Sens.," 14(2), 337, 2022. <https://doi.org/10.3390/rs14020337>
- [8] A. Baibagysoy, A. Magiera, N. Thevs and R. Waldhardt, "Resource Characteristics of Common Reed (*Phragmites australis*) in the Syr Darya Delta, Kazakhstan, by Means of Remote Sensing and Random Forest," Plants, 2025. <https://www.mdpi.com/2223-7747/14/6/933>
- [9] P. Grabusts, J. Musatovs and Ē. Teirumnieka, Modeling the Distribution of Lake Reeds Using GIS, In Proceedings of the 16th International Scientific and Practical Conference Environment. Technology. Resources, Rezekne Latvia, June 2025. <https://doi.org/10.17770/etr2025vol2.8619>
- [10] “Latvian lakes database.” [Online] Available: <https://www.ezeri.lv/database/2196/> [Accessed: Feb. 20, 2026].
- [11] “Copernicus project,” [Online] Available: <https://www.copernicus.eu/en> [Accessed: Feb. 20, 2026].
- [12] “SentiWiki Home Page,” [Online] Available: <https://sentiwiki.copernicus.eu/web/sentiwiki> [Accessed: Feb. 20, 2026].
- [13] “QGIS project,” [Online] Available: <https://qgis.org/project/overview/> [Accessed: Feb. 20, 2026].
- [14] R.O. Duda, P.E. Hart and D.G. Stork, Pattern Classification, 2nd edition, 2001.
- [15] S.Haykin, Neural Networks and Learning Machines, 3rd edition, Pearson, 2009.
- [16] L. Breiman, Random Forests. Machine Learning, 45(1), 5–32, 2001. <https://doi.org/10.1023/A:1010933404324>
- [17] C.M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.

Decision-Making Dynamics in Secure Software Development Teams: The Role of AI-Supported Systems

Boris Gramchev

Department of Industrial Management
Technical University of Varna
Varna, Bulgaria
gramchev@gmail.com

Marina Marinova-Stoyanova

Department of Industrial Management
Technical University of Varna
Varna, Bulgaria
mpmstoyanova@tu-varna.bg

Abstract—The increasing integration of AI into secure software development is reshaping technical processes and decision-making within teams. While existing research has focused on performance and detection capabilities, less attention has been given to how AI influences the human aspects of decision formation. This study examines how AI-supported security tools affect decision-making dynamics among software developers and security specialists. Using a quantitative survey-based approach, the study explores relationships between trust in AI, transparency, perceived usefulness, team coordination, and decision confidence. The findings show that AI does not directly determine decision outcomes, but operates through socio-cognitive mechanisms, with trust emerging as the central driver of decision confidence. Transparency contributes indirectly by supporting trust, while team coordination strengthens the integration of AI-generated insights into collective decisions. Perceived usefulness functions mainly as a baseline condition for adoption rather than a determinant of outcomes. The study highlights a key implication: AI-supported systems may increase decision confidence without improving decision quality. By framing AI-supported decision-making as a socio-technical process, this research clarifies how AI reshapes not only what decisions are made, but how they are constructed within teams.

Keywords— *Artificial Intelligence; Decision Confidence; Secure Software Development; Team Coordination; Trust.*

I. INTRODUCTION

The growing integration of artificial intelligence into software development has begun to reshape not only how systems are built, but also how decisions are made within development teams. Nowhere is this shift more visible than in security-critical environments, where the identification and prioritization of vulnerabilities increasingly rely on AI-supported tools. These systems analyze large volumes of code, detect anomalies, and generate recommendations [1], [2] that directly influence how risks are assessed and addressed. While their technical capabilities are well documented, less attention has been given to how they affect the human side of decision-making, particularly in

team-based settings where security decisions are rarely made in isolation [3], [4].

Secure software development has traditionally depended on a combination of expertise, judgment, and coordination among developers and security specialists. Decisions about vulnerabilities are often complex, time-sensitive, and context-dependent, requiring not only technical analysis but also interpretation and negotiation within the team. The introduction of AI-supported systems alters this process by inserting algorithmically generated recommendations into the decision flow. These recommendations do not simply provide additional information; they shape how problems are framed and how attention is allocated. As a result, decision-making becomes increasingly mediated, raising important questions about how teams interpret, trust, and act upon AI-generated insights [5], [6].

Despite the rapid adoption of AI in software security, existing research has largely focused on performance improvements, detection accuracy, and system capabilities. Comparatively little empirical work has examined how AI-supported tools influence decision-making dynamics within teams [7], [8]. This represents a critical gap, as the effectiveness of AI in practice depends not only on its technical performance but also on how it is embedded within social and organizational processes. In particular, factors such as trust in AI, perceived transparency of recommendations, and the quality of team coordination may significantly shape how AI outputs are interpreted and used [7], [9].

This study addresses this gap by examining how AI-supported security tools influence decision-making within secure software development teams. The focus is not on whether AI improves detection accuracy, but on how it affects the process through which decisions are formed. Specifically, the study investigates three interrelated questions: how AI-supported tools influence decision-making processes within teams, how developers and security specialists interpret AI-generated

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.132>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

recommendations, and which factors determine the effective integration of these recommendations into collective decision-making. By focusing on trust, transparency, perceived usefulness, and team coordination, the study seeks to capture the key mechanisms through which AI reshapes decision dynamics.

Conceptually, the study is grounded in the view that AI-supported decision-making is a socio-technical process, where technological outputs interact with human judgment and team interaction. Prior research on human-AI collaboration suggests that AI systems do not replace decision-making but reconfigure it by altering how information is structured and how authority is distributed [10], [11]. At the same time, research on trust in AI highlights that users' willingness to rely on algorithmic recommendations depends less on technical accuracy alone and more on perceived reliability and contextual understanding [7]. These perspectives suggest that the impact of AI on decision-making is mediated through human and relational factors rather than being directly determined by system capabilities.

Based on this reasoning, the study adopts a model in which transparency contributes to the formation of trust, trust influences decision confidence, and team coordination shapes how individual judgments are translated into collective decisions. Perceived usefulness is treated as a baseline condition that supports adoption but does not directly determine decision outcomes. Rather than formalizing these relationships as strict hypotheses, the study takes an exploratory empirical approach, aiming to identify patterns and relationships within real-world data. This choice reflects the emerging nature of the research area, where rigid hypothesis testing may be less appropriate than capturing the structure of interactions between variables.

The contribution of this study is twofold. First, it provides empirical evidence on how AI-supported systems influence decision-making dynamics in secure software development, moving beyond a purely technical perspective. Second, it offers a conceptual framework that highlights the role of trust, transparency, and coordination as key mechanisms in AI-mediated decision processes. By doing so, the study contributes to a more nuanced understanding of how AI reshapes not only what decisions are made, but how they are formed within teams.

II. AI IN SECURE SOFTWARE DEVELOPMENT

The integration of artificial intelligence into secure software development has accelerated significantly in recent years, reshaping how vulnerabilities are detected, assessed, and prioritized [2], [1]. What was once a largely manual and experience-driven process is now increasingly supported by systems capable of analyzing large volumes of code, identifying patterns, and generating security recommendations in real time. These tools promise not only efficiency gains but also a shift toward more proactive and continuous security practices embedded directly within the development lifecycle [4].

At a functional level, AI is most visibly applied in vulnerability detection. Machine learning models are used to identify known patterns of insecure code, detect anomalies, and flag potential risks that might be overlooked by human reviewers [1]. Unlike traditional rule-based systems, these models can adapt to new data and improve over time, making them particularly valuable in environments where threats evolve rapidly. However, this capability also introduces new forms of uncertainty, as the logic behind detections is often probabilistic rather than deterministic, making it less transparent to users [9].

Beyond detection, AI increasingly plays a role in risk assessment and prioritization. Modern security tools do not simply list vulnerabilities; they rank them, estimate their potential impact, and suggest remediation strategies [1]. In doing so, they move from being passive tools to active participants in the decision-making process. This shift is subtle but important. When a system not only identifies a vulnerability but also recommends what should be addressed first, it begins to shape the decision space itself. Teams are no longer evaluating raw information but interacting with pre-structured judgments generated by the system.

This evolution aligns with broader developments in decision-support systems, where AI is positioned as an augmentation layer rather than a replacement for human expertise [6]. In theory, this augmentation allows teams to combine computational power with human contextual understanding, leading to more informed decisions. In practice, however, the balance between automation and human control is not always stable. As AI systems become more capable, there is a tendency for users to rely more heavily on their outputs, sometimes without fully questioning them. This creates a dynamic where efficiency increases, but critical scrutiny may decrease.

One of the defining characteristics of AI-supported security tools is their ability to operate at scale. They can process vast amounts of code and security data far beyond human capacity, enabling continuous monitoring and near real-time feedback. This is particularly valuable in agile and DevOps environments, where rapid iteration cycles require equally rapid security assessments. AI makes it possible to integrate security checks directly into development pipelines, supporting the idea of "security by design" rather than security as a separate phase [3].

At the same time, the integration of AI into development workflows introduces new challenges related to interpretability and trust. Developers and security specialists must decide how much to rely on AI-generated recommendations, often without full visibility into how those recommendations were produced [12]. This issue becomes more pronounced in complex models, where the reasoning process is not easily accessible. As a result, the effectiveness of AI tools depends not only on their technical accuracy but also on how they are perceived and understood by users [8].

Another important dimension is the interaction between AI systems and team-based work structures. Secure

software development is rarely an individual activity; it involves coordination between multiple roles, including developers, security engineers, and managers. AI tools introduce shared reference points in the form of alerts, scores, and recommendations, which can facilitate communication but can also create new dependencies. Teams may begin to rely on AI outputs as common ground for discussion, which can streamline coordination but may also limit the diversity of viewpoints if those outputs are not critically examined [13].

Recent research [2] also highlights the importance of human oversight in AI-supported security processes. While AI can identify patterns and suggest actions, it lacks contextual awareness and cannot fully account for organizational priorities, trade-offs, or strategic considerations. Human judgment remains essential in interpreting AI outputs and making final decisions. This reinforces the idea that AI should be understood as part of a broader socio-technical system rather than as a standalone solution [11].

Furthermore, the use of AI in security raises concerns related to bias, reliability, and overreliance. Models trained on historical data may reproduce existing biases or fail to detect novel types of vulnerabilities. False positives and false negatives remain a challenge, and overconfidence in AI outputs can lead to missed risks. These limitations do not negate the value of AI but highlight the need for balanced use, where automation is complemented by critical evaluation and continuous validation [14].

Taken together, these developments suggest that AI is transforming secure software development not only at the level of tools but at the level of processes and decision structures. It changes what information is available, how it is interpreted, and how decisions are made within teams. This transformation sets the stage for examining how these changes influence decision dynamics, particularly in terms of trust, transparency, and coordination, which become central factors in determining how AI-supported systems are actually used in practice.

III. TEAM DECISION DYNAMICS IN AI-MEDIATED ENVIRONMENTS

Decision-making in secure software development has traditionally been a collective and iterative process, shaped by technical expertise, risk awareness, and situational context. The introduction of AI-supported systems changes this process in a more subtle but fundamental way. AI does not simply make analysis faster or detection more accurate. It changes how information is formed, how it is interpreted, and how it is validated within teams. As a result, decision-making becomes mediated, moving from a purely human activity toward a hybrid form of interaction where responsibility and judgment are shared between people and systems [5].

A key shift occurs in the nature of decision inputs. Previously, teams relied on direct interpretation of logs, alerts, and contextual signals. With AI, this information is already filtered, prioritized, and framed before it reaches

the team. What appears as input is, in reality, already an interpretation. AI systems highlight what seems important and implicitly suggest what should be done next [13]. This creates efficiency, but it also subtly shapes how problems are understood. Team members are more likely to anchor their reasoning around AI outputs, which can guide attention while at the same time limiting alternative perspectives [10], [6].

This anchoring effect has visible consequences in team interactions. When AI outputs are seen as credible, they help teams move faster and reduce uncertainty. Discussions become more focused, and decisions can be reached with less friction. At the same time, this speed can come at a cost. Teams may converge too quickly on AI-supported conclusions, not because all alternatives have been explored, but because the recommendation already feels sufficiently justified. In high-pressure environments, this tendency becomes even stronger, creating a tension between efficiency and critical evaluation [8].

Trust becomes the central mechanism through which this tension is managed. In AI-mediated environments, trust extends beyond interpersonal relationships to include the system itself. Whether a recommendation is accepted or challenged depends largely on how reliable the system is perceived to be. In many cases, users cannot fully understand how AI outputs are generated, especially when models are complex or opaque [10]. In such situations, trust fills the gap left by limited understanding. Teams act not because they fully comprehend the reasoning, but because they believe the system is dependable [7].

The role of transparency is therefore more complicated than it might initially appear. While it is often assumed that more explanation leads to better decisions, this is not always the case. Detailed explanations can improve understanding, but they can also increase cognitive load or create confusion, especially when team members have different levels of expertise. In practice, the same explanation may be interpreted differently across individuals, which can introduce misalignment rather than clarity. Transparency, therefore, does not directly improve decisions, but works through trust and interaction within the team [15], [16].

Team coordination is equally important in this process. Security decisions are inherently collaborative, requiring input from developers, security specialists, and other stakeholders. AI systems introduce shared reference points, such as alerts and risk scores, which can support alignment. However, coordination does not happen automatically. The meaning of AI outputs still needs to be discussed, negotiated, and aligned across the team. Different roles, experiences, and expectations can lead to different interpretations of the same recommendation, making communication a critical part of the decision process [13].

Seen in this way, decision-making unfolds across several interconnected layers. At the informational level, AI structures what is visible and what is prioritized. At the cognitive level, individuals interpret these signals based on trust, experience, and perceived usefulness. At the

relational level, teams align their interpretations and arrive at shared decisions. The effectiveness of the overall process depends on how well these layers work together. Weakness in any one of them can disrupt the entire decision dynamic.

Importantly, AI does not replace human judgment but repositions it. The focus shifts from analyzing raw data to interpreting AI-generated representations of that data [1]. This shift carries risks. AI outputs may appear objective, but they are shaped by underlying assumptions, training data, and design choices that are not always visible to users. As a result, teams may rely on recommendations that carry hidden biases or limitations [14].

Another consequence is the emergence of dependency. As teams rely more on AI for prioritization and risk assessment, they may engage less with the underlying data. While this improves efficiency, it can reduce critical thinking and limit the diversity of viewpoints within the team. Over time, this may lead to more uniform decisions, but not necessarily better ones. This is particularly problematic in security contexts, where adaptability and critical judgment are essential [2].

Overall, decision-making in AI-supported environments is best understood as a socio-technical process. Its effectiveness depends not only on the capabilities of AI systems, but also on how they are interpreted, trusted, and integrated into team interactions. By focusing on trust, transparency, and coordination, this study captures the key mechanisms through which AI reshapes decision dynamics and sets the stage for examining their impact on decision outcomes.

IV. RESEARCH METHODOLOGY

This study adopts a quantitative research design to examine how AI-supported security tools influence decision-making dynamics within secure software development teams. Given the exploratory nature of the research questions and the need to capture perceptions, attitudes, and behavioral tendencies across different roles, a structured survey approach was selected as the most appropriate method. Survey-based research has been widely used in studies examining technology adoption, trust in automated systems, and team-level processes, as it allows for the systematic measurement of latent constructs such as trust, perceived usefulness, and decision confidence [16], [17]. This approach is particularly relevant in the context of human-AI collaboration, where decision-making emerges from the interaction between algorithmic recommendations and human judgment [5].

The empirical setting of the study focuses on software developers and security specialists working in security-sensitive development environments. These include professionals involved in vulnerability detection, threat assessment, and secure coding practices, where AI-supported tools are increasingly integrated into daily workflows. A total of 96 participants were included in the study, representing a balanced mix of technical roles. Approximately 62% of respondents identified as software developers, while 38% reported primary responsibilities in cybersecurity or security engineering. The average

professional experience among participants was 5.8 years, indicating a sample with sufficient exposure to both traditional and AI-supported development practices.

Data collection was conducted through an online questionnaire designed to capture key dimensions of AI-supported decision-making. All items were measured using a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5), allowing for consistent quantification of subjective perceptions. The questionnaire was structured to ensure clarity and accessibility, avoiding overly technical language while maintaining conceptual precision. Prior to distribution, the instrument was reviewed and refined to ensure internal consistency and face validity. Each construct was measured using two items adapted to the context of AI-supported security tools, ensuring both conceptual clarity and measurement consistency.

The study examines five core variables that reflect both technological and team-level aspects of decision-making in AI-supported environments. Trust in AI-supported tools captures the extent to which participants perceive AI-generated recommendations as reliable and accurate. In AI-mediated environments, trust plays a critical role in determining whether algorithmic outputs are accepted, questioned, or ignored within team decision processes [7]. Decision confidence reflects the degree to which AI tools enhance individuals' certainty when making security-related decisions. Perceived usefulness assesses the practical value of AI tools in improving vulnerability detection and prioritization processes. AI transparency refers to the extent to which the reasoning behind AI-generated outputs is understandable and interpretable. Finally, team coordination captures how effectively team members align their actions and interpretations when AI-generated insights are introduced into the decision process.

Decision confidence was selected as the dependent variable as it represents the most immediate and measurable outcome of AI-supported decision-making at the individual level. In the context of secure software development, objective decision quality is difficult to assess directly within a survey-based design, particularly given the complexity and context-specific nature of security incidents. As a result, decision confidence serves as a proximal indicator of decision outcomes, reflecting the extent to which individuals feel assured in their judgments when interacting with AI-generated recommendations. This choice is consistent with prior research on technology-supported decision-making, where confidence is often used as an operational proxy for decision effectiveness in situations where objective performance measures are not readily observable. However, it is important to acknowledge that decision confidence does not necessarily imply decision accuracy, a distinction that is further addressed in the discussion of the findings.

To ensure the reliability of the measurement model, internal consistency was assessed using Cronbach's alpha. All constructs demonstrated satisfactory reliability, with values ranging between 0.78 and 0.85, exceeding commonly accepted thresholds for exploratory research

[18]. These results indicate that the measurement scales are sufficiently stable for subsequent analysis.

The analytical approach combines descriptive statistics, correlation analysis, and multiple regression modeling to examine relationships between variables. Correlation analysis was used to identify the strength and direction of associations between key constructs, while regression analysis was employed to test the predictive effects of trust, transparency, and coordination on decision confidence. In addition, a moderation analysis was conducted to explore whether team coordination strengthens the relationship between trust in AI and decision confidence. This approach allows for a more nuanced understanding of how individual perceptions and team processes interact in shaping decision outcomes.

Overall, the methodological design provides a structured yet flexible framework for capturing the interplay between AI-supported systems and team-level decision dynamics. By combining established measurement approaches with a focused set of variables tailored to secure software development, the study offers a credible empirical basis for examining how AI influences not only technical processes but also the social and cognitive mechanisms underlying collective decision-making.

While the preceding sections provide the conceptual background for understanding AI-supported decision-making, the primary contribution of this study lies in the empirical examination of how trust, transparency, coordination, and perceived usefulness shape decision confidence in secure software development teams.

V. RESULTS

The empirical analysis provides direct evidence regarding the mechanisms through which AI-supported systems influence decision-making within secure software development teams. Overall, the findings indicate that AI tools are perceived as valuable contributors to security-related processes, but their influence is not uniform across variables. The results reveal a differentiated structure in which trust emerges as the dominant driver of decision confidence, while transparency and team coordination play more supportive roles.

Descriptive statistics are presented in Table 1. Perceived usefulness reports the highest mean, indicating that participants clearly recognize the functional value of AI tools in vulnerability detection and prioritization. Trust in AI and decision confidence also show relatively strong levels, although with greater variability, suggesting differences in how individuals evaluate and rely on AI-generated recommendations. Team coordination demonstrates moderately positive levels, while transparency remains comparatively lower, indicating that understanding the reasoning behind AI outputs is still a partial limitation.

TABLE 1. DESCRIPTIVE STATISTICS OF STUDY VARIABLES

Variable	M	SD
Trust in AI	3.85	0.81
Transparency	3.63	0.77
Decision Confidence	3.82	0.85
Team Coordination	3.76	0.68
Perceived Usefulness	3.95	0.68

To examine the relationships between variables, Pearson correlation analysis was conducted. The results, shown in Table 2, indicate that all variables are positively related, although with varying strength. Trust in AI demonstrates a strong positive association with decision confidence, confirming its central role in shaping how confident individuals feel when making security-related decisions. Transparency is also moderately associated with both trust and decision confidence, suggesting that interpretability contributes to decision-making, but not as a dominant factor.

Team coordination shows a positive but more moderate relationship with decision confidence compared to initial expectations, indicating that while coordination supports decision processes, its influence may be more contextual than direct. Perceived usefulness is positively related to all variables, particularly trust, but the strength of these relationships remains moderate, suggesting that usefulness functions more as a background condition than a primary driver. Overall, the correlation pattern supports the structure of the proposed model, while also indicating differences in the relative weight of each variable.

TABLE 2. PEARSON CORRELATIONS AMONG VARIABLES ($p < .01$)

Variable	1	2	3	4	5
Trust in AI	1.00				
Transparency	0.62**	1.00			
Decision Confidence	0.68**	0.55**	1.00		
Team Coordination	0.24**	0.23**	0.40**	1.00	
Perceived Usefulness	0.41**	0.33**	0.43**	0.23**	1.00

To further test the predictive relationships, a multiple regression analysis was conducted with decision confidence as the dependent variable. The results are presented in Table 3. Trust in AI emerges as the strongest predictor, with a substantial and highly significant effect, indicating that perceived reliability of AI-generated recommendations is the primary factor shaping decision confidence.

Team coordination also demonstrates a significant positive effect, although weaker than trust, suggesting that collective processes still play an important role in reinforcing confidence, even if their direct influence is more limited than initially assumed. In contrast, transparency does not reach conventional levels of statistical significance, indicating that while interpretability

contributes to trust, it does not independently drive decision confidence when other variables are considered simultaneously.

The overall model explains a substantial proportion of variance in decision confidence, confirming that the selected variables capture key aspects of AI-supported decision-making dynamics, while also highlighting the dominant role of trust over other factors. The model explains approximately 56% of the variance in decision confidence ($R^2 = .559$).

TABLE 3. MULTIPLE REGRESSION ANALYSIS PREDICTING DECISION CONFIDENCE (DEPENDENT VARIABLE: DECISION CONFIDENCE)

Predictor	β	SE	p
Trust in AI	0.50	0.10	< .001
Transparency	0.17	0.10	0.082
Team Coordination	0.27	0.09	< .01
Perceived Usefulness	0.16	0.10	0.095

To further examine the role of team processes, a moderation analysis was conducted focusing on the interaction between trust in AI and team coordination. The results indicate a statistically significant interaction effect (see Table 4), suggesting that the relationship between trust and decision confidence becomes stronger in teams characterized by higher levels of coordination. In such contexts, AI-generated insights are more effectively integrated into shared decision processes, amplifying their impact. In contrast, in less coordinated teams, trust alone is less sufficient to produce high levels of decision confidence.

TABLE 4. MODERATION ANALYSIS: INTERACTION EFFECT. (DEPENDENT VARIABLE: DECISION CONFIDENCE)

Predictor	β	SE	p
Trust in AI	1.34	0.48	< .001
Team Coordination	1.02	0.50	< .05
Trust $\times$ Coordination	0.18	0.13	< .05

An additional pattern emerges with respect to perceived usefulness. Although it is positively associated with other variables, it does not reach statistical significance in the regression model. This suggests that perceived usefulness may function primarily as a baseline condition for adoption rather than as a direct determinant of decision outcomes. While participants appear to recognize the practical value of AI tools, this recognition does not consistently translate into higher decision confidence or more effective decision-making.

To assess the potential risk of common method bias, Harman's single-factor test was conducted using all measurement items. The results indicate that the first unrotated factor accounts for 45.40% of the total variance, which is below the commonly accepted threshold of 50% (see Table 5). This suggests that common method bias is

unlikely to pose a serious threat to the validity of the findings.

TABLE 5. HARMAN'S SINGLE-FACTOR TEST RESULTS

Component	% of Variance Explained	Cumulative %
1	45.40	45.40
2	12.08	57.48
3	9.60	67.08
4	7.97	75.05
5	5.82	80.87

Taken together, the findings point to a more differentiated structure of AI-supported decision-making than initially assumed. Trust in AI-supported systems emerges as the central mechanism, while coordination plays a supporting role and transparency functions primarily as an indirect contributor. Rather than replacing human judgment, AI appears to reshape how confidence is constructed and how decisions are collectively validated within secure software development teams.

VI. DISCUSSION

The empirical findings provide several insights into the role of AI-supported systems in secure software development teams. Rather than confirming a purely technology-driven view of decision-making, the results suggest that human and team-level factors remain central in determining how AI-generated recommendations are interpreted and used.

The findings of this study offer a more nuanced understanding of how AI-supported systems influence decision-making within secure software development teams. While prior expectations often emphasize the technical capabilities of AI tools, the results here suggest that their impact is primarily shaped by human interpretation, trust, and team interaction rather than by functionality alone.

The most prominent finding is the central role of trust in AI-supported systems. Across both correlation and regression analyses, trust emerges as the strongest predictor of decision confidence, indicating that the perceived reliability of AI-generated recommendations is the key mechanism through which these tools influence decision-making. This reinforces the idea that AI does not directly determine decisions but instead operates through human acceptance. When developers trust the outputs, they are more willing to rely on them, integrate them into their reasoning, and act upon them. Without such trust, even technically accurate systems may fail to influence decisions in meaningful ways.

In contrast, transparency plays a more limited role than initially assumed. Although it is positively associated with both trust and decision confidence, its effect becomes statistically weak when other variables are considered simultaneously. This suggests that while understanding AI-generated outputs contributes to the formation of trust, it

does not independently drive decision confidence. In practical terms, teams may rely on AI recommendations even when they do not fully understand how they are produced, as long as those recommendations are perceived as reliable. This finding challenges the common assumption that explainability is always a primary driver of effective AI use and instead positions it as a supporting rather than leading factor.

Team coordination also contributes to decision confidence, although its effect is more moderate than expected. The results indicate that coordination strengthens the integration of AI-generated insights into decision processes, particularly in teams where communication and alignment are already well established. The moderation analysis further supports this interpretation, showing that the relationship between trust and decision confidence becomes stronger in more coordinated teams. This highlights that AI tools do not operate in isolation but are embedded within social systems where their influence depends on how information is shared, discussed, and collectively interpreted.

An important implication of these findings is the distinction between decision confidence and decision quality. While the results clearly show that AI-supported systems increase confidence, this does not necessarily mean that decisions are objectively better. In fact, it is possible that AI tools create a sense of assurance that is not always matched by improved outcomes. This introduces a potential risk in AI-supported environments, where increased confidence may reduce critical evaluation and lead to overreliance on automated recommendations. In this sense, AI may reshape not only how decisions are made, but also how they are perceived and justified within teams.

The role of perceived usefulness further supports this interpretation. Although participants recognize the practical value of AI tools, usefulness does not emerge as a significant predictor of decision confidence. This suggests that functional benefits alone are insufficient to explain how AI influences decision-making. Instead, usefulness appears to function as a baseline condition for adoption, while trust and coordination determine how AI is actually used in practice.

Taken together, these findings point to a layered model of AI-supported decision-making. At the foundational level, usefulness enables adoption. At the interpretive level, transparency contributes to trust. At the cognitive level, trust shapes individual confidence. Finally, at the collective level, team coordination determines how effectively this confidence is translated into shared decisions. This layered structure emphasizes that the impact of AI in secure software development is not purely technological but deeply social and cognitive.

From a practical perspective, the results suggest that organizations should focus not only on improving the technical performance of AI tools, but also on fostering trust and strengthening team coordination. Efforts to increase transparency should be balanced with the

recognition that interpretability alone may not drive effective use. Instead, the challenge lies in integrating AI systems into team processes in a way that supports informed, reflective, and collectively validated decision-making.

A further limitation of the study relates to the sample size, which may limit the statistical power to detect interaction effects. While the sample is sufficient for the main regression analysis, larger samples would be required to more reliably assess moderation relationships in future research.

VII. CONCLUSION

This study set out to examine how AI-supported tools influence decision-making within secure software development teams, shifting the focus from technical performance to the human and team-level dynamics that shape actual outcomes. The findings show that the impact of AI is not direct, but mediated through trust, interpretation, and coordination. Among the examined factors, trust in AI-supported systems emerges as the strongest driver of decision confidence, highlighting that the effectiveness of AI depends less on its capabilities alone and more on how it is perceived and accepted by users.

At the same time, transparency and perceived usefulness, while relevant, do not independently determine decision outcomes. Instead, they contribute indirectly by supporting trust and facilitating interpretation. Team coordination further strengthens the integration of AI-generated insights, emphasizing that decision-making remains a collective process even in highly automated environments. An important implication is that increased confidence does not necessarily imply improved decision quality. AI systems can create a sense of certainty that may not always be justified, introducing potential risks of overreliance. Overall, the study demonstrates that AI in secure software development functions as part of a broader socio-technical system. Its effectiveness depends not only on technological sophistication but on how it is embedded within human judgment and team interaction.

REFERENCES

- [1] Kaur, R., Gabrijelčić, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- [2] Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing artificial intelligence. *MIS Quarterly*, 45(3), 1433–1450. <https://doi.org/10.25300/MISQ/2021/16274>
- [3] Binns, R. (2022). Human judgement in algorithmic loops: Individual justice and automated decision-making. *Regulation & Governance*, 16(1), 197–211. <https://doi.org/10.1111/rego.12358>
- [4] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- [5] Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J. M. (2019). Hybrid intelligence. *Business & Information Systems Engineering*, 61, 637–643. <https://doi.org/10.1007/s12599-019-00595-2>
- [6] Faraj, S., Pachidi, S., & Sayegh, K. (2018). Working and organizing in the age of the learning algorithm. *Information and*

- Organization*, 28(1), 62–70.
<https://doi.org/10.1016/j.infoandorg.2018.02.005>
- [7] Glikson, E., & Woolley, A. W. (2020). Human Trust in Artificial Intelligence: Review of Empirical Research. *Academy of Management Annals*, 14, 627–660.
<https://doi.org/10.5465/annals.2018.0057>
- [8] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- [9] Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human–AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577–586.
<https://doi.org/10.1016/j.bushor.2018.03.007>
- [10] Kaur, D., Uslu, S., Rittichier, K. J., & Durresi, A. (2022). Trustworthy artificial intelligence: A review. *ACM Computing Surveys*, 55(2), 1–38. <https://doi.org/10.1145/3491209>
- [11] McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, 2(2), 1–25.
<https://doi.org/10.1145/1985347.1985353>
- [12] Nguyen, T. T., & Reddi, V. J. (2023). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*, 34(8), 3779–3795.
<https://doi.org/10.1109/TNNLS.2021.3121870>
- [13] Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review*, 46(1), 192–210.
<https://doi.org/10.5465/amr.2018.0072>
- [14] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*, 10(6), 1473–1498.
<https://doi.org/10.1007/s40745-022-00444-2>
- [15] Ameh, J. E., Otebolaku, A., Shenfield, A., Ikpehai, A., & Sule, D. (2025). *Machine learning approaches in software vulnerability detection: A systematic review and analysis of contemporary methods* [Preprint]. *Research Square*.
<https://doi.org/10.21203/rs.3.rs-5975490/v1>
- [16] Suresh, H., Gomez, S. R., Nam, K. K., & Satyanarayan, A. (2021). Beyond expertise and roles: A framework to characterize the stakeholders of interpretable machine learning and their needs. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 74, 1–16.
<https://doi.org/10.1145/3411764.3445088>
- [17] Tahaei, M., Vaniea, K., & Rashid, A. (2023). Embedding Privacy Into Design Through Software Developers: Challenges and Solutions. *IEEE Security & Privacy* 21(1), 49–57.
<https://doi.org/10.1109/MSEC.2022.3204364>
- [18] Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. *Applied Artificial Intelligence*, 38(1).
<https://doi.org/10.1080/08839514.2024.2439609>

Generalized Net Model of the Disaster Protection Assessment Process Using Artificial Intelligence

Rosen Iliev

Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
r.iliev@di.mod.bg

Svilen Neykov

Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
svilen@nkv.me

Abstract: The paper presents an original generalized net model (GN-model) for using artificial intelligence in assessing the protection of the population and infrastructure in disasters. It includes assessments of basic components such as population, infrastructure, personnel and procedures using intuitionistic fuzzy logic. A simulation of the GN-model was conducted in the GN IDE simulation environment and some of the results obtained are presented. Possible applications of the model for improving the procedures for protecting the population and infrastructure in disasters and accidents are described.

Keywords: AI, crisis, generalized net, model

I. INTRODUCTION

Managing the protection of the population in disasters and accidents is a major challenge for modern society due to the unexpectedness of the event, the scope of damage, uncertainty, sometimes the inadequacy of the measures taken and, last but not least, the lack of experience. By applying modern technologies and innovative solutions using UAS to obtain information, this process can be significantly facilitated, since traditional algorithms have difficulty dealing with uncertainty, and here artificial intelligence (AI) comes to the rescue for processing large streams of sensor data and for rapid analysis of the situation.

The paper presents an innovative approach to modeling crisis management through a hybrid GN-AI architecture, including the integration of information extraction tools (UASs, satellites, sensors, social networks, etc.), their processing through artificial intelligence (primary data analysis, computer vision for destruction, sensor analysis), modeling through Generalized Nets (GN) and the use of solutions based on large language models (LLM) such as Chat-GPT, Gemini, etc., for semantic interpretation and generation of generalized operational information in natural language to the crisis headquarters.

For a more precise assessment of the characteristics of objects in conditions of uncertainty typical of crisis situations, the use of Intuitionistic Fuzzy Logic (IFL) is

proposed, which extends Zadeh's fuzzy logic (FL) and allows the use of more parameters for assessment - in addition to the degree of belonging (μ), also the degree of non-belonging (ν) and uncertainty (π). The application of other modeling networks, such as N-nets (a variation of Petri nets), is used in [1]. Other publications related to the modeling and analysis of threats to information systems can be seen in [2, 3, 4].

II. MATERIALS AND METHODS

HYBRID GN-AI ARCHITECTURE TO SUPPORT CRISIS MANAGEMENT

The integration of Generalized Nets (GN) and Artificial Intelligence (AI) through a multi-agent architecture Multi-Agent System (MAS) enables the construction of a dynamic, self-learning system. Specialized AI agents analyze data streams in real time (terrain sensors and drones for seismic activity, use of hydrological and meteorological models for probable floods, etc.), and through prediction algorithms based on the use of Convolutional Neural Networks (CNN), anomalies are identified before they develop into a critical event. In a critical situation, AI agents can optimize travel routes in real time and avoid closed or dangerous evacuation routes. The use of Generalized Nets allows for more flexible modeling of different objects, subjects and resources (teams, population, infrastructure, logistics, etc.) because they can integrate different tools (methods, algorithms, fuzzy evaluation functions, etc.) for more precise modeling. GN can be presented as the backbone of such a hybrid architecture for modeling the process, including the following components:

1. Perception Layer (AI)

The use of CNN for real-time camera image analysis (identification of destroyed infrastructure) is important for predicting possible threats to the population, as they automate the "vision" of drones, transforming the visual stream into specific information about the damage [5].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.142>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

CNNs support the process of identifying damaged infrastructure in the following ways:

1) Automated recognition of specific defects

CNNs are designed to recognize visual patterns (edges, shapes, and textures) in a manner similar to human vision, but at much higher speed [6]. Models such as YOLO (You Only Look Once) can identify cracks in concrete, exposed reinforcement, or missing elements of bridges and buildings in real time [7]. CNNs can perform damage classification by degree (e.g., from slight surface defects to complete structural collapse), which helps prioritize rescue operations [8].

2) Real-time analysis

Integrating optimized CNN models directly into drone hardware allows data to be processed on-site (Edge computing) instead of waiting for data to be transmitted to a central server [9]. This is achieved with traffic mapping: drones can immediately mark blocked roads or collapsed bridges on a virtual map of the area, guiding rescue teams along safe routes. Speed of response is also important: AI models achieve accuracy of over 90-95%, processing thousands of frames in minutes – a task that would take a human team hours [10].

3) Semantic terrain segmentation

Unlike simple object detection, architectures such as U-Net or SegNet perform terrain segmentation pixel by pixel. This means that AI can accurately delineate the boundaries of flooded areas or the area of collapsed buildings, which is very useful for timely calculation of the necessary resources for restoration [11].

4) Threat detection in adverse conditions

CNNs can be combined with various sensors (thermal cameras, LiDAR) to see through smoke or at night. This allows thermal analysis to identify structural damage through temperature anomalies (e.g. hot water leaks or short circuits), as well as to ignore “noise” – well-trained neural networks can distinguish a crack in concrete from ordinary shadow or vegetation, avoiding false alarms [12].

The integration of CNNs into generalized nets allows for great scalability – hundreds of drones can simultaneously scan a huge area, with each agent (MAS) sending only the most important information about critical damage to the crisis center.

2. Natural Language Processing (NLP)

In disaster situations, the flow of information from social networks and telephone lines is huge and chaotic. NLP for analyzing signals from citizens and social networks turns this chaos into structured data. NLP technologies serve to filter and structure informal communication from the population by automating text analysis (social networks, SMS, chatbots) to extract critical data about the location and type of incident, which allows MAS agents to reallocate resources to the hottest spots in real time. Some of these capabilities are as follows:

1) Automatic classification of NLP models, such as BERT or RoBERTa – allows for quick recognition of the

type of incident in a text message (e.g. “fallen person”, “flood”, “fire”). This allows the system to automatically prioritize some incidents over others and direct specialized teams according to the specific situation. A study on how transformation models (BERT) filter out the “noise” in social networks to extract only emergency signals can be found in [13] and [14].

2) Named Entity Recognition (NER) – the algorithms allow the extraction of named objects and recognize names of streets, neighborhoods or landmarks in informal texts (e.g. “near “Eagle Bridge”). This allows the automatic mapping of signals on the map, even in cases where GPS coordinates are not sent [15].

3) Sentiment Analysis and Panic Detection (Sentiment Analysis) – by analyzing the emotional charge of messages, authorities can identify outbreaks of disinformation. This helps to direct psychological support teams or send refuting messages to calm the population [16].

4) Summarization – a very important task that AI can easily handle if there are thousands of tweets or posts published about a single event. In this case, NLP models create a short summary for operators: “The bridge in the north is impassable, over 200 people are reporting it.” This saves time for dispatchers, who do not have to read thousands of individual messages [17].

3. Decision Layer

One possibility to support decision-making in crisis situations is to use AI agents for dynamic resource allocation through Reinforcement Learning (RL). Here, the agent is trained to allocate resources (personnel, rescue teams) in a simulation environment. In this training, the AI agent makes a series of decisions in a dynamic simulation environment through a mechanism of “rewards and punishments”. In the context of crisis management, this approach is used to optimize logistics and the allocation of critical personnel in real time [18]. Unlike traditional static algorithms, RL agents can navigate complex scenarios with high uncertainty, adapting to sudden changes in the infrastructure to minimize response time [19].

Another possibility is the application of Intuitionistic Fuzzy Logic (IFL) in the management of generalized nets, where it is a natural extension of the Theory of Generalized Nets, developed by Acad. Atanassov. Unlike standard fuzzy logic, IFL takes into account not only the degree of membership (μ), but also the degree of non-membership (ν) and uncertainty (π), which is critical in the situation of unexpected disasters (e.g. “we are not sure if this road is destroyed”).

The application of IFL in the predicates of the transitions of generalized nets is not new, but it allows modeling of situations with a high degree of uncertainty and uncertainty, characteristic of natural disasters [20]. While standard fuzzy logic takes into account only the degree of truth, IFL introduces additional parameters for the degree of falsehood and the degree of fluctuation (volatility) [21]. Within a GN, these logical predicates serve as “intelligent filters” that assess the reliability of incoming information from sensors and citizens, making

critical decisions to redirect resources even in the presence of contradictory or incomplete data [22].

4. Execution Layer

The execution layer (evacuation and protection procedures) represents the final phase in the architecture of the multi-agent system, where the decisions made are translated into physical actions to protect the population. Within the framework of the generalized net process modeling, this layer coordinates the work of autonomous evacuation agents that guide citizens along dynamically calculated safe routes (focusing on emergency evacuation path planning, which is the core of the “Execution Layer”) [23]. The effectiveness of the evacuation is ensured by real-time data integration, which allows the execution mechanisms to avoid high-risk areas and infrastructure damage. In this regard, [24] presents a mathematical model of how agents simulate and execute evacuation in an urban environment. This layer encompasses both digital early warning systems and the physical deployment of resources to limit the consequences of the disaster. [25] discusses collaborative governance and how decisions are assigned to executive units.

DESCRIPTION OF THE GN MODEL WITH AI COMPONENTS

The generalized net structures the overall process, and the AI modules and IFL are integrated into the network and determine the values in the transition matrices. Tokens are not just data, but objects, subjects, resources, infrastructure, procedures, etc., with characteristics (embedding vectors), which are filled in by the data received from sensors after processing by AI modules. The predicates in the transitions are not fixed logical conditions, but results of neural networks (for example: “If the probability of a dam collapse is $> 40\%$, direct the token to an alternative route”).

The GN model is characterized by the use of dynamic characteristics, i.e. the AI module acts as a function for updating the characteristics of certain tokens. Each time they pass through a corresponding transition, the AI module “adds” new information to the token’s memory. The model also includes a Learning Loop so that the results (success/failure) can be fed back to the AI module for further training (Feedback loop), which makes the GN model more adaptive.

Components with AI integration include:

a) Infrastructure Component (AI for computer vision)

Here, the GN model receives data from sensors and cameras. The role of AI is to use pretrained models (e.g. YOLO or ResNet) for image segmentation. The transition in the GN model analyzes the state of critical infrastructure (roads, hydroelectric power plants, power grid). If the AI detects an anomaly, the Infrastructure token changes its characteristic to Compromised, which automatically triggers resource redirection in the next transition (through the corresponding predicate rules).

b) “Personnel” component (AI for optimization)

Here, AI is used to solve tasks such as “Resource Allocation”, and Reinforcement Learning (RL) or Genetic Algorithms can be used for this purpose. When a “Disaster” call arrives, the AI module calculates the optimal number of teams and their composition (doctors, firefighters, engineers) based on the complexity of the situation. The model monitors the workload of the staff in real time (according to the assigned tasks) to prevent fatigue.

c) “Procedures” component (AI for decision-making support)

Here, the role of AI is to support the decision-making process with incomplete information using IFL. The predicates in the matrix are not hard (0 or 1), but depend on membership and non-membership functions (e.g. “the water level is high”, “the wind speed is critical”). This component decides which procedure from the “Protection Plans” to activate, with AI assessing the risk and selecting the appropriate procedure (evacuation, isolation or rescue), minimizing potential casualties. The integration of AI and IFL into predicates (so-called Fuzzy Predicates) allows for more accurate assessments by using fuzzy rules, for example: IF (intensity is “High”) AND (passability is “Low”) THEN (Activate “Air Rescue”). When using IFL, AI models (e.g. neural networks) do not simply provide a classification, but generate IFL values for the characteristics of the token: For example, the AI image analysis module (CNN) scans drone footage and assigns the corresponding token a score (0.7, 0.2) for a given bridge (70% probability of being healthy, 20% of being collapsed, 10% ambiguity due to smoke/clouds). The AI population analysis module analyzes population density and cell data to determine the severity of the situation in a given sector.

Description of GN transitions

The schematic of the model implemented with the generalized GN net is shown in Fig. 1, and the description is as follows:

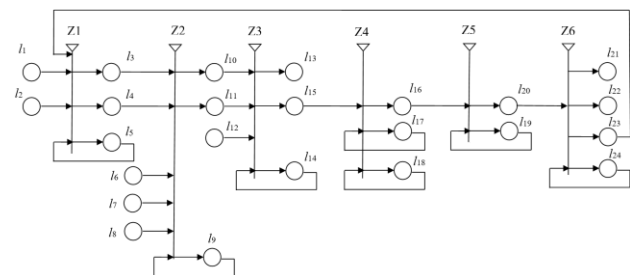


Fig. 1. GN-model of the disaster protection assessment process using AI

$$GN = \{Z1, Z2, Z3, Z4, Z5, Z6\}$$

The model kernels (tokens) used in a generalized net GN are:

- Token α_s (Sensor Data): Initial feature: “raw terrain data” (signals, images, river levels, etc.). AI converts this into “disaster intensity”.
- Token α_i (Infrastructure): Feature (μ_i, v_i) – degree of functionality and degree of destruction of roads/facilities – bridges, hospitals).

- Token α_P (Rescue Team Personnel/Resources): Feature (μ_c, v_c) – response capacity and degree of exhaustion/risk (also “availability, location and capacity of rescue teams”).

- Token α_D (Decision/Actions): Generated in the simulation process as the final result (action plan).

- Token α_{Pop} (Population/People in distress): Feature (μ_p, v_p) – degree of threat and safety. Example: (0.7, 0.2) means a highly endangered population with 20% certainty in their survival and 10% complete uncertainty (information deficit).

As can be seen, each token carries an IFL score of the type (μ, v) , where $\mu+v \leq 1$, as well as specific characteristics that are updated when passing through the transitions. When the transitions in the GN-model function using IFL predicates, each transition is triggered if the “degree of truth” for the incoming token exceeds a certain threshold. Below, only the more essential elements of the GN-model will be described – positions occupied by the tokens and predicates used.

Transition Z1: Intelligent perception (Perception Layer)

Here, AI modules process the raw data. The processing is carried out using classical algorithms for computer vision and pattern recognition. At the input positions, tokens α s with terrain data received from sensors located on the site (at position l_1) or from specialized UASs (at position l_2) arrive. The transition matrix contains predicates whose values are generated by AI. Neural networks analyze the flow of tokens and as a result, the tokens receive initial IFL estimates, for example: if AI “sees” smoke, but is not sure whether it is fire, it assigns a high uncertainty π , according to IFL.

Transition Z2: Risk Assessment Layer

This is the most important transition, where the needs of the population and the possibilities for providing assistance meet. It includes the tokens α_{Pop} (population, people in distress), α_I (infrastructure), α_P (rescue teams, resources) and α_S (sensor data). Using IFL predicates, the degree of risk (criticality) for people is calculated in relation to the state of the environment and the possibilities for evacuation.

Input positions:

- l_6 : Token α_{Pop} (with an IFL criticality degree (μ_p, v_p))
- l_7 : Token α_P (with an IFL capacity degree (μ_c, v_c))
- l_8 : Token α_I with infrastructure passability data (with an IFL assessment (μ_c, v_c))

Output positions:

- l_9 : for processing and waiting, monitoring (wait)
- l_{10} : for providing assistance on site (relief)
- l_{11} : for active evacuation (evac)

Predicate $W_{9,11}$: „Need for immediate evacuation“. $W_{9,11}$ is true if the AI population threat estimate $\mu(\alpha_{Pop}) >$

0.7 and the uncertainty $\pi(\alpha_{Pop}) < 0.2$. If the predicate is true, the token α_{Pop} moves to the “Evacuation” position (l_{11}).

Transition matrix:

	l_9	l_{10}	l_{11}
l_3	$W_{3,9}$	False	False
l_4	$W_{4,9}$	False	False
l_6	$W_{6,9}$	$W_{6,10}$	$W_{6,11}$
l_7	$W_{7,9}$	$W_{7,10}$	$W_{7,11}$
l_8	$W_{8,9}$	$W_{8,10}$	$W_{8,11}$
l_9	$W_{9,9}$	$W_{9,10}$	$W_{9,11}$

Predicates (calculated by AI and IFL):

- $W_{3,9}$ and $W_{4,9}$ “If the AI analysis of the token with sensor data μ_S obtained from Z1 requires “processing” in transition Z2”.

- $W_{6,9}$ and $W_{6,10}$ “If the AI analysis of the population μ_{Pop} requires “waiting” (for $W_{6,9}$) or “providing assistance on site” (for $W_{6,10}$).

- $W_{6,11}$: “If the AI population threat assessment $\mu_p > 0.8$ and the uncertainty $\pi_p < 0.15$ ” (there is a critical need for evacuation).

- $W_{7,9}$ and $W_{7,10}$ “If the staff capacity μ_c requires “waiting” (for $W_{7,9}$) or “providing assistance on site” (for $W_{7,10}$).

- $W_{7,11}$: “If the staff capacity μ_c allows for transportation”.

- $W_{8,9}$ and $W_{8,10}$ “If the AI analysis of the infrastructure μ_{infra} requires “wait” (for $W_{8,9}$) or “provide on-site assistance” (for $W_{8,10}$).

- $W_{8,11}$: “If the AI analysis of the population μ_{Pop} confirms a safe route”.

- $W_{9,9}$, $W_{9,10}$ and $W_{9,11}$ “If the AI analysis requires “wait” (for $W_{9,9}$), “provide on-site assistance” (for $W_{9,10}$) or “active evacuation” (for $W_{9,11}$) respectively (processing process).

Transition Z3: Resource and infrastructure analysis (Intelligent Analysis Layer)

Here it is decided which resources are fit for use.

The AI component includes a neural network (e.g. CNN) that analyzes data from α_I and α_P to determine the probability of survival of infrastructure objects. The input positions are l_{10} (infra_status) – infrastructure status, l_{11} (staff_status), l_{12} (staff_input) – increase in rescue teams and l_{14} (process) – processing information about the situation, and the output positions are l_{13} – terminal position for failed tokens and l_{15} – transition position for admitted tokens to the next transitions.

The main predicates are the following:

- $W_{10,15}$ (road_ok): “The road is passable for heavy equipment” (result of AI analysis of satellite images).

- $W_{11,15}$ (staff ready): “The team is in combat readiness” (fatigue/logistics forecast model).

Transition Z4 Aid distribution Layer

When passing through this transition, the tokens acquire new characteristics through the IFL evaluation operator, such as: The population token (α_{pop}) acquires a new characteristic $F=(\mu_{new}, v_{new})$, where μ_{new} is the degree of successful aid distribution (removal from danger).

The AI module calculates the fluctuation index $\pi=1-(\mu+v)$. If π is too high (e.g. above 0.4), the model automatically generates a token-request for “Additional Air Reconnaissance” (via position l_{23} of transition Z6). In this transition, α_{pop} (affected population) α_p (personnel) and α_i (infrastructure) meet, and an optimization algorithm (e.g. Genetic) that works with IFL weights can be used. This allows the rescue team to be selected for which the characteristic μ (readiness) is maximized and v (risk to the team) is minimized.

This transition takes the data from the environment and classifies it.

Input positions: l_{15} (tokens with data).

Output positions: l_{16} – position occupied by tokens that have successfully passed the transition (α_{pop} with acquired new characteristics), l_{17} (process-risk_low), l_{18} (process-risk_high) – for determining the degree of risk.

Transition matrix:

	l_{16}	l_{17}	l_{18}
l_{15}	False	True	True
l_{17}	$W_{17,16}$	$W_{17,17}$	False
l_{18}	$W_{18,16}$	$W_{18,17}$	$W_{18,18}$

where $W_{17,16}$, $W_{17,17}$, $W_{18,16}$, $W_{18,17}$ and $W_{18,18}$ are predicates calculated by the AI risk assessment module.

Transition Z5: Generation of a decision-making procedure (Decision Making Layer)

This transition is the interface between the model and the human operator. It coordinates everything in a single plan. The AI module is an agent that seeks to minimize a loss function (victims, time).

Predicate $W_{16,19}$ (refine): “If the uncertainty π is too high”. Then the token returns to the beginning of the network (via position l_{23} of transition Z6) to collect additional data (new feature: “needs verification”).

Predicate $W_{19,20}$ (final): “If the trust index of the DSS system is above the threshold τ (e.g., $\mu - v > 0.5$)”. Then the token moves on to the next transition Z6 (for preparing a draft order of the crisis center). If successful, the token receives the characteristic: “Evacuation plan along Route X with team Y”.

The DSS module may include a knowledge base (protection rules based on legal regulations and past experience), IFL (a mathematical apparatus that compares intuitionistic fuzzy assessments of different plans) and a

visualization panel (Dashboard) for visualization of a “Risk Map” with areas of security (μ) and degree of uncertainty (π).

Transition Z6: Cognitive Interface (LLM Layer)

This is the final transition of the model. Here enter the cores carrying processed data from the previous transitions. Digital data is converted into meaningful sentences using LLM (for example, (0.9, 0.05) into “Critical situation in Zone B, immediate evacuation!”). In this transition, a task list is generated for the teams (Step-by-step) and dynamic maps (Heatmaps) can be generated in real time for the monitors in the crisis center.

The LLM is defined as a function of the characteristics of the final token that enters the transition. The transition Z6 accepts the token α_D (Decision) that entered the network from the DSS system through position l_{12} , and the LLM accepts the data from the previous transitions as a context (Prompt) and generates natural language. For each decision in the model, an Intuitionistic Fuzzy Hesitation Index is calculated: $\pi = 1-(\mu+v)$. If the LLM finds, for example, that $\pi > 0.4$ (too many unknowns), the model automatically returns the token back to Z1 for “Additional Intelligence” (through position l_{23}) before confirming the evacuation order.

Input for the LLM: IRL estimates from the transitions (μ , v , π), the state of the “Population” token and the capacity of “Personnel”.

LLM Output: Synthesized report like: “In area B there is an 85% risk of flooding, evacuation is difficult due to a collapsed bridge (uncertainty 15%). Recommendation: Air rescue.”

Action plan: Outlined steps for rescue teams.

Possible generation of scripts (e.g. in Python) to draw interactive maps in the crisis center.

III. RESULTS AND DISCUSSION

SIMULATION OF THE GN MODEL IN THE GN IDE SIMULATION ENVIRONMENT

By using the GN IDE (Generalized Nets Integrated Development Environment) simulation environment, different scenarios can be set and how the process is modeled in different crisis situations can be studied. One example of this is reducing the evacuation time and more efficient use of the infrastructure (quantitative indicators) in a specific flood simulation scenario. In this case, the cores enter the input positions of the network (transition Z1) and in the processing process (through position l_5) the AI module supplies data on rising waters. IFL filters the uncertain data received from the sensors and initially processed by the AI module. Further, other cores enter the network for assessing the infrastructure, for personnel (rescuers), etc., and at transition Z5 DSS suggests evacuation routes. The language model (LLM) at transition Z6 prepares a visualization of the data with a media release and an evacuation plan.

Some steps of the model simulation process with GN IDE can be seen in Fig. 2.

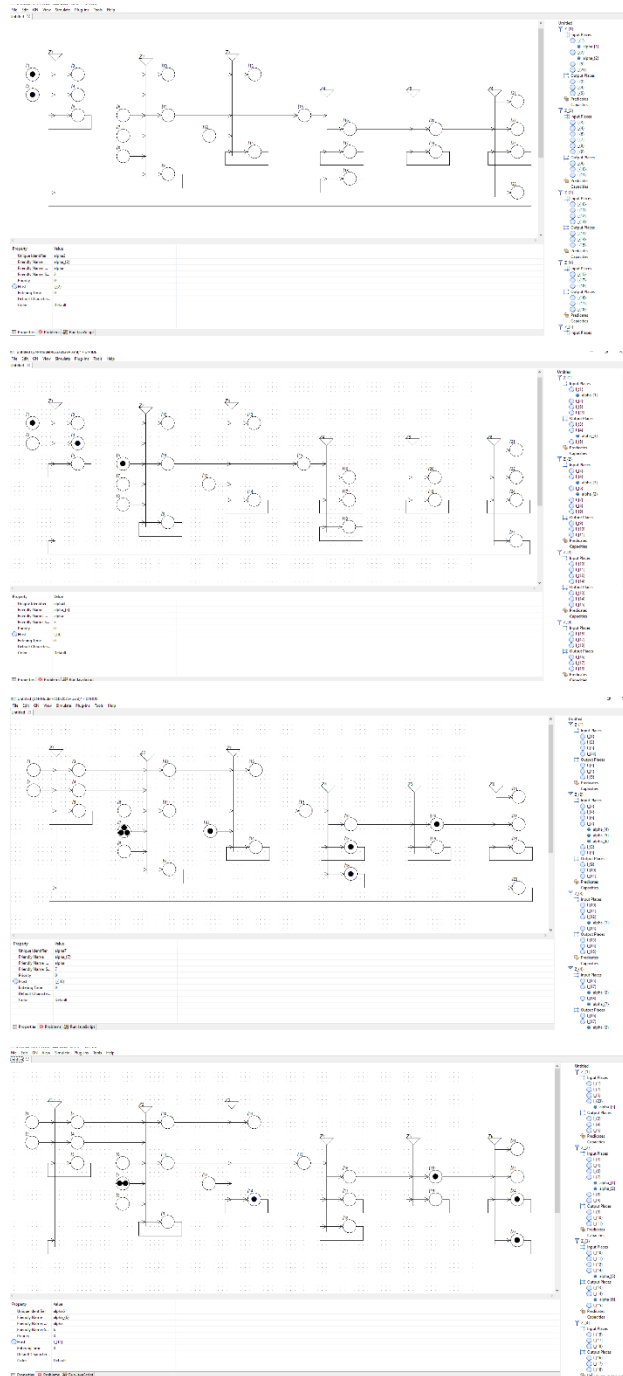


Fig. 2. Screens from the GN model in the GN IDE simulation environment

The application of AI and GN-modeling is increasingly being used in various fields, one of which is national security and defence. This area has been the subject of intensive work in recent years and many scientific studies have been conducted, such as in [26, 27, 28].

IV. CONCLUSION

The presented original GN-model with AI-support to support the crisis management process is an attempt to

expand the application of generalized models in an integrated approach of sensor data (obtained from UASs and from the local area), information processing through AI-modules (agents) and the application of language models (LLM) for communication with the crisis headquarters in natural human language. The use of IFL in the evaluation functions of the tokens that move in the generalized net provides an additional opportunity for more detailed modeling of the data processing process in the presence of uncertain information, which is characteristic of the complex conditions of the crisis situation. An important element is also the attempt to transition from static plans to "Dynamic Procedures", which are adapted in real time by trained AI-models. This is perhaps the first attempt to integrate Deep Learning into the framework of Generalized Civil Protection Nets, by creating a single methodological framework, combining the rigor of GN with the flexibility of AI and reducing the subjective factor ("human error") for the initial damage assessment.

V. ACKNOWLEDGMENT

This work was supported by the NSP "Security and defence" program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

- [1] V. Tselkov, and N. Stoianov. E-net models of a software system for web pages security. Mathematics and mathematical education, Sofia, Bulgaria, BAS, 2003.
- [2] P., Boyanov, Using a specialized software for comprehensive monitoring the suspicious states in computer networks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 6, 2014, pp. 148-154.
- [3] Hr. Hristov, P. Boyanov, and T. Trifonov. Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 101-107.
- [4] A. Kolev, and P. Nikolova, Instrumental Equipment for Cyber-attack Prevention, Information & Security: An International Journal 47, no. 3 (2020): 285-299.
<https://doi.org/10.11610/isij.4720>
- [5] "What is AI-powered damage detection in drone inspections?," FlyNex FAQ. [Online]. Available: <https://www.flynex.io/en/faq-items/what-is-ai-powered-damage-detection-in-drone-inspections/>
- [6] "CNN Dimov," ICT-BAS Publications. [Online]. Available: https://sdp.iict.bas.bg/publ/CNN_Dimov.pdf
- [7] "Article Title," arXiv preprint arXiv:2510.21063, 2025.
<https://doi.org/10.48550/arXiv.2510.21063>
- [8] "Article Title," arXiv preprint arXiv:2510.21063, 2025. [Online]. Available: <https://arxiv.org/abs/2510.21063>
- [9] IEEE Xplore Document. [Online]. Available: <https://ieeexplore.ieee.org/document/11101106>
- [10] ScienceDirect Article. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0045794925001191>
- [11] MDPI Remote Sensing Article. [Online]. Available: <https://www.mdpi.com/2072-4292/17/15/2668>
- [12] "Drone digital twins for structural damage assessment," Anvil Post. [Online]. Available: <https://anvil.so/post/drone-digital-twins-for-structural-damage-assessment>

- [13] "Article Title," arXiv preprint arXiv:2510.21063, 2025. <https://doi.org/10.48550/arXiv.2510.21063>
- [14] R. P. Westerholt, P. Resch, and A. Zipf, "A statistical approach to the use of social media data in disaster management," *Sci. Rep.*, vol. 11, no. 1, p. 14231, Jul. 2021 Available: <https://nature.com>
- [15] J. R. Curran and S. Clark, "Language-independent NER using a maximum entropy combined model," in *Proc. ACL Workshop on Computational Learned Lexical Semantics*, Stanford, CA, USA, 2014. [Online]. Available: stanford.edu
- [16] S. Behl, A. Rao, S. Aggarwal, S. Chadha, and H. S. Pannu, "Resource optimization for disaster management using Twitter data processing," *Int. J. Disaster Risk Reduct.*, vol. 34, pp. 29–42, Mar. 2019. Available: <https://www.sciencedirect.com/science/article/pii/S2212420918306630>
- [17] UN OCHA, "Artificial Intelligence for Disaster Response: Current Trends and Future Perspectives," *ReliefWeb Report*, Oct. 2021. [Online]. Available: reliefweb.int.
- [18] Y. S. Bagloee, M. Sarvi, and M. Patriksson, "A Reinforcement Learning Application for Real-Time Emergency Resource Allocation," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18234–18245, Oct. 2022 Available: <https://ieeexplore.org>
- [19] X. Liang, et al., "Deep Reinforcement Learning for Dynamic Resource Allocation in Disaster Response Networks," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013567
- [20] K. T. Atanassov, *Intuitionistic Fuzzy Sets*, Heidelberg, Germany: Physica-Verlag, 1999. Available: <https://springer.com>
- [21] K. T. Atanassov, *On Generalized Nets*, Singapore: World Scientific, 1991. Available: <https://worldscientific.com>
- [22] V. Bureva, S. Sotirov, and E. Sotirova, "Generalized Net Model of Disaster Management with Intuitionistic Fuzzy Predicates," in *Proc. 21st Int. Conf. on Intuitionistic Fuzzy Sets (ICIFS)*, Sofia, Bulgaria, 2017, pp. 64–70.
- [23] M. Biçer and V. K. Akram, "Multi-Agent Based Path Planning for Emergency Evacuation in Smart Cities," in *Proc. IEEE 13th Int. Conf. on Semantic Computing (ICSC)*, Newport Beach, CA, USA, 2019, pp. 412–417.
- [24] X. Chen and Y. Zhan, "Agent-Based Modeling and Simulation of Urban Evacuation under Disaster Scenarios," *IEEE Access*, vol. 8, pp. 21563–21575, 2020. Available: <https://ieeexplore.org>
- [25] F. S. Hsieh, "Collaborative Disaster Management Based on Multi-Agent Systems," in *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC)*, Bari, Italy, 2019, pp. 2454–2459. doi: 10.1109/SMC.2019.8914364
- [26] Manchev A. I. "Ammunition Supply In Multinational Joint Operations", In: *International Scientific Conference – Hemus-2020*, pp. I-111–118, ISSN 1213-2916, Plovdiv, Bulgaria, 2020
- [27] Ivanov V. V. Manchev A. I. "Crises And Some Possibilities For Their Successful Management", In: *Proceedings of the International Scientific Conference - ARTDef*, (29-30 June 2021), pp. I-86–93, ISSN 2815-2581 Varna, Bulgaria, 2021
- [28] Ivanov V. V., Manchev A. I. "Opportunities For Improving The National Security System Of The Republic Of Bulgaria", In: *Proceedings of the International Scientific Conference – Hemus - 2022* (2-3 June 2022), pp. VI-123–133, ISSN 1213-2916, Sofia, Bulgaria, 2022.

Electronic Evidence in Criminal and Civil Proceedings: Technologies, Challenges and Perspectives

Sandra Kaija

Rīga Stradiņš University
Rīga, Latvia,
ORCID 0000-0002-2711-613X

Inga Kudeikina

Rīga Stradiņš University
Rīga, Latvia
ORCID 0000-0002-7895-4264

Abstract. In the contemporary digital environment, electronic evidence has become a fundamental element in both criminal and civil proceedings. The accelerated evolution and pervasive integration of information technologies into routine activities, communication, and business processes has led to a substantial augmentation in the volume and significance of digital data as potential evidence. This evolution has created a pressing need for a coherent, consistent, and technologically informed legal framework to regulate the collection, preservation, evaluation, and admissibility of electronic evidence in judicial proceedings.

Notwithstanding the ongoing evolution of the legal landscape, the utilisation of electronic evidence continues to be encumbered by a plethora of intricate challenges. These include the authentication, integrity, and reliability of digital data, as well as the mitigation of risks associated with data manipulation, cybersecurity threats, and cross-border data access. Furthermore, discrepancies in procedural regulations between criminal and civil proceedings have the potential to result in inconsistencies in the handling and assessment of electronic evidence.

The present article undertakes a comparative analysis of the legal framework governing electronic evidence in both criminal and civil contexts, with a view to identifying common principles and key distinctions. Furthermore, it delves into pertinent jurisprudence, emphasising existing regulatory lacunae and practical challenges that emerge in the implementation of legal standards within technologically sophisticated settings.

The objective of the present article is twofold. Firstly, the present study seeks to analyse the current legal regulation of electronic evidence and its alignment with technological realities. Secondly, it evaluates the challenges encountered during its application and proposes directions for improvement. It is imperative to emphasise the importance of enhancing legal certainty, procedural fairness, and the effective integration of technological solutions in evidence handling processes. The study emphasises the necessity of a balanced approach that ensures both the reliability of electronic evidence and the protection of fundamental rights in judicial proceedings.

The present study employs a combination of descriptive, analytical, deductive and inductive methods. The descriptive method is utilised to present the nature of electronic evidence, the legal and technical details of its acquisition and use. The analytical method is employed to examine in depth the existing laws and regulations and their interpretation in jurisprudence, and to identify problems. Deductive and inductive methods are used to express conclusions and suggestions. The deductive method is employed to analyse the application of general rules in specific situations involving electronic evidence, while the inductive method is used to formulate general conclusions and recommendations for improving the legal framework for electronic evidence by examining specific court rulings and legal experts' findings.

Keywords – *electronic evidence, admissibility of evidence, technologies, digital forensics*

I. INTRODUCTION

In the digital age, electronic evidence assumes an increasingly pivotal role in both criminal and civil proceedings. Technological advancements in the realm of information creation, storage, and transmission are profoundly reshaping the landscape of justice. Consequently, legal systems worldwide are confronted with substantial challenges in ensuring the reliability, admissibility, and effective utilisation of electronic evidence within judicial processes.

The term 'electronic evidence' encompasses a vast array of digital data, including emails, text messages, social media content, metadata, cloud-stored files, and information extracted from electronic devices. In contradistinction to conventional forms of evidence, digital data is highly volatile, readily alterable or deleteable, and necessitates specialised forensic techniques to ensure its integrity and authenticity. Consequently, courts and legal practitioners must adapt to the complexities of handling such evidence while maintaining fundamental legal

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.98>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

principles, such as fairness, due process, and the protection of individual rights. Despite the existence of legal frameworks regulating electronic evidence, various challenges persist. These include inconsistencies in legislation, difficulties in cross-border data access, privacy concerns, and the need for clear guidelines on admissibility criteria. Furthermore, the rapid evolution of technology raises ongoing questions about how legal norms should be adjusted to address new forms of digital evidence, such as blockchain records, artificial intelligence-generated data, and encrypted communications.

The objective of this article is to analyse the current legal regulation of electronic evidence and its alignment with technological realities, while also evaluating the challenges encountered in its application and propose possible directions for improvement. By assessing existing laws, court practices, and expert opinions, this research seeks to provide valuable insights into how electronic evidence can be more effectively integrated into the judicial process.

II. ELECTRONIC EVIDENCE – REGULATORY CHALLENGES

The right to a fair trial is considered a fundamental human right by both international law and the national law of every democratic country. Evidence plays an important role in ensuring this right, although there is no uniform legal definition of the concept of "proof". Its content must be disclosed in the context of an analysis of procedural law. For instance, Section 127, Paragraph one of the Criminal Procedure Law stipulates that "evidence in criminal proceedings is any information obtained in accordance with the procedures prescribed by law and corroborated in a specific procedural form regarding facts [...]" [16], while Section 92, Paragraph one of the Civil Procedure Law states that "evidence is information on the basis of which the court determines the existence or absence of facts which are relevant for the adjudication of the case" [3]. A literal interpretation of the term leads to the conclusion that, more broadly, the term "evidence" is used in the legal protection system to designate anything used to prove that something else is true or exists, from witness statements to documents, objects, etc. [21].

The legislation does not provide for a predetermined set of items of information to be regarded as evidence. The court retains the prerogative to determine the admissibility of evidence, through the application of quantitative and qualitative analysis to news reports. This position has been endorsed by the Senate of the Republic of Latvia, which has asserted that the evaluation of evidence falls within the purview of the court [18].

Simultaneously, it is important to acknowledge that the legislature did not entrust the evaluation of the evidence to the court's discretion, but rather delineated the criteria to be fulfilled when assessing the submitted information. In other words, the information becomes evidence when it fulfils the specified criteria. It is imperative to acknowledge that the evaluation of evidence is not left to the court's discretion, but rather, it is subject to specific criteria that must be met for its admissibility in court proceedings.

These criteria, outlined in sections 130 of the Criminal Procedure Law and 95 of the Civil Procedure Law, serve to ensure the integrity and reliability of the evidence presented. Consequently, it can be concluded that the assessment of evidence is a cognitive process, constituting a legal act undertaken by the court through the application of principles of logic and law. In terms of its internal content, this process may be described as a "limited free" assessment of evidence, in the sense that, on the one hand, the court is not constrained by external conditions in its assessment of evidence and, on the other hand, the court is bound by the requirements of the legislation. In this regard, Mr Bukovsky, a legal scholar, has articulated the following: "On the one hand, it does not restrict the judiciary in the assessment of evidence and, on the other hand, obliges the court to go into the substance of each piece of evidence in detail by comparing it with others and gives it the weight it deserves in terms of its internal value" [2].

In the contemporary digital age, electronic evidence has become an increasingly prominent aspect in both criminal and civil proceedings. This encompasses a wide range of digital data, including emails, text messages, social network records, metadata, files, and IP addresses, among others. However, the utilisation of this evidence poses a number of technical and legal challenges. These challenges pertain to the authenticity, integrity, and procedural requirements of the evidence, as well as the substantial complexity involved in assessing it.

The legal framework does not distinguish electronic evidence in civil proceedings as a specific category of evidence, nor does it define it as a separate legal institute, thus giving rise to questions regarding its assessment. We concur with the position espoused in the scientific literature that an equality mark cannot be affixed between the assessment of electronic evidence and the assessment of "paper" evidence [17]. Dr.iur. D. Ose also expressed a similar view with regard to electronic evidence in civil proceedings, stating that "the rules relating to the understanding and submission of written evidence no longer meet the needs of modern proceedings" [20].

The Criminal Procedure Law, conversely, has already recognised electronic evidence as a form of evidence since 2025, as outlined in Section 136 of the Law. This stipulates that evidence in criminal proceedings may encompass information on facts in the form of electronic information processed, stored or transmitted by automated data processing equipment or systems.

The necessity to enhance the legal framework is predicated on several factors, including the perceived absence of a legal definition in the Civil Procedure Act and the recognition that the creation, storage and handling of digital data may pertain not only to the alleged author of the data itself, but also to third parties who, in many cases, may not even be subject to the jurisdiction of the country in which the proceedings are taking place. For instance, if a photograph from a Facebook profile is submitted as evidence, but the defendant claims that his account was hacked and the photograph is fake or generated by artificial

intelligence, the court may encounter difficulties in determining its authenticity and admissibility as evidence. Researcher Juris Balodis-Boluge has highlighted the challenges posed by the absence of a definitive electronic evidence definition. Through a thorough evaluation of multiple court judgments, he has arrived at the conclusion that "in one criminal case, the court recognises data discs with communication control records as material evidence, in another criminal case the court recognises the evidence of a similar nature – a data disc with video control record – as an electronic document, but in another criminal case the court recognises such data discs as electronic evidence" [1]. The absence of a definition, in itself, would not pose a problem unless it resulted in a further negative impact on legal certainty due to the use of technology. The lack of regulation, i.e. technologies as such, does not have a single legal framework covering all areas and aspects. Instead, there is a multi-layered and fragmented framework that depends on the technology in question, its purpose and legal context. Legal regulation of technologies takes place at several levels: 1) At the international level, conventions, treaties and EU regulations that establish general guidelines. The international framework for electronic evidence is founded on several significant documents, including: the Budapest Convention on Cybercrime – the inaugural international document that established fundamental principles for the collection and exchange of electronic evidence among nations; and the EU Regulation on the European electronic evidence order [11] – which stipulates procedures for obtaining electronic evidence from providers of online services, from other EU countries; the General Data Protection Regulation (GDPR) – which regulates the processing of personal data and affects the storage and use of electronic evidence in judicial proceedings; 2) at regional level – for example, directives and regulations on data protection, artificial intelligence, cyber security, etc. are adopted at EU level. The EU Artificial Intelligence Act and the E-evidence Regulation [10] represent the primary legislative instruments in this regard. At the national level, each country establishes its own legal framework, which may align with international regulations but often exhibits significant variations. For instance, in the Republic of Latvia, the national framework for the utilisation of electronic evidence is encompassed within multiple legal acts: The Criminal Procedure Law stipulates the circumstances in which information obtained and utilised as electronic evidence in criminal proceedings is admissible. The Civil Procedure Law, while not explicitly providing for the use of electronic evidence, is relevant in this context as it establishes the framework for the administration of justice in the Republic of Latvia; despite the absence of explicit provisions in the Civil Procedure Law concerning the utilisation of electronic evidence in civil proceedings, the law does not inherently prohibit such practices. For instance, it permits the use of electronic evidence as a form of written evidence. However, the Personal Data Processing Act serves to complement the requirements stipulated in the GDPR, thereby imposing limitations on the processing of electronic evidence.

The basis for the assessment of electronic evidence consists of four well-established principles: 1) No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court; 2) In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions; 3) An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result; 4) The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to [13].

Whilst not seeking to question the necessity of the principles, it is important to note that their declaratory nature may be problematic in practice. There is a lack of standardised procedures, which hinders the collection and analysis of high-quality electronic evidence [19].

It is further noteworthy that the regulatory issues concerning electronic evidence are more pertinent to criminal proceedings. In contrast, civil proceedings, characterised by their adversarial nature, are driven by individual interests, which in practice renders the acquisition and verification of electronic evidence even more challenging. A significant challenge lies in the limited capacity for international cooperation. The legal framework for the taking of evidence abroad in civil matters is delineated by Regulation (EC) No 1206/2001 of the Council of the European Union of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil and commercial matters. The scientific literature has expressed the view that "one of the problems in practice is the identification of the lengthy and heavy-handed procedure in which the question in question (question of taking evidence — aut. note) is decided, i.e. Article 10 of Regulation (EC) No 1206/2001 provides that the requested court shall execute the request immediately or at the latest within 90 days of receipt of the request" [20].

It is important to note that the complexity of evaluating electronic evidence is not and cannot be decisive for its admissibility. The court's primary responsibility is to ensure the authenticity of electronic evidence, and consequently, its admissibility. Electronic evidence cannot be refused on the basis of its complex examination process. This assertion is supported by scientific literature, which acknowledges that electronic means of proof are analogous to traditional means and that electronic evidence does not constitute a novel form of evidence, but rather a novel technology-based verification mechanism for proof [12].

The EncroChat case [4] has become one of the most significant judgments in the European Union dealing with issues of electronic evidence collection, use and admissibility in criminal proceedings. This judgment underlines the need to clarify the boundaries between legitimate investigations and mass electronic surveillance. In the EncroChat case, law enforcement used digital infiltration to obtain encrypted communications that were

seen as evidence of criminal activity. However, the collection of such mass data, which also affects persons not involved in criminal activities, raised questions about respect for the right of individuals to privacy, as guaranteed by the Charter of Fundamental Rights of the EU and the European Convention on Human Rights, as well as about judicial supervision and control mechanisms necessary to prevent illegal or disproportionate behaviour by public authorities.

The CJEU emphasised that national courts must ensure that electronic evidence is obtained and used in accordance with EU and national law, particularly with respect to the fundamental right to privacy and to a fair trial. The Court underscored that the mass acquisition of electronic data, including the hacking of encrypted communication tools, is permissible only if it is carried out in accordance with the principles of proportionality and necessity, ensuring effective judicial control.

In the context of this Article, it is imperative to emphasise that one of the most salient issues in the EncroChat case was whether the data thus obtained may be the primary evidence in criminal proceedings. The Court observed that the procurement of evidence must be conducted in accordance with procedural regulations and the safeguarding of human rights; defendants must be capable of verifying the provenance and authenticity of the evidence, a task that can prove challenging in technically intricate cases; if the evidence is obtained unlawfully or infringes fundamental rights, it may be deemed inadmissible in court, particularly if it constitutes the sole or decisive basis of the accusation. These aspects assume particular significance given the use of EncroChat data in several European countries as pivotal evidence in the prosecution of criminal organisations.

The EncroChat case demonstrates significant legal and procedural challenges related to the acquisition and use of electronic evidence, emphasising the necessity for clear legal frameworks and legal oversight mechanisms to ensure fair legal action and privacy protection in the digital age. While laws and regulations establish principles for the use of electronic evidence, case law in this field is still developing in Latvia, highlighting the need for more detailed regulations regarding authentication, storage, and procedures for the use of evidence. The international exchange of electronic evidence frequently poses challenges related to the protection of jurisdiction and privacy, particularly when data is stored in foreign territories. These issues are set to become increasingly prevalent in national courts, as evidenced by the Norwegian Supreme Court's 28 March 2019 decision [22] concerning the conduct of searches at a company in relation to alleged computer fraud. The investigation involved a request for permission to conduct a search at the company's office in Oslo to access data stored on servers overseas that could provide information about the alleged fraud. The Supreme Court ruled that such a search did not violate the exclusive executive jurisdiction of other countries because the

coercive measure was initiated in Norwegian territory against a Norwegian company with offices in Norway.

III. TECHNOLOGICAL METHODS FOR CORROBORATING ELECTRONIC EVIDENCE

The utilisation of electronic evidence within legal proceedings necessitates the employment of specialised methodologies, the purpose of which is to ensure its authenticity, integrity and legal admissibility. Digital forensics, a term not explicitly defined in legislation, is nevertheless regarded as a method in its own right. However, it is important to note that the content of digital forensics should be distinguished from the general norms of the Criminal Procedure Law regarding the procedures by which evidence is obtained and used, as well as the legal force of the Electronic Documents Law, which prescribes the use of electronic documents [7]. These legal provisions are of particular relevance in the context of digital forensics.

Digital forensics can thus be defined as a set of systematic methods and technologies used to identify, obtain, analyse and preserve electronic evidence while ensuring its integrity and admissibility in legal proceedings. It covers a wide range of processes, from data recovery to forensic analysis, and is used in both judicial investigations and cybersecurity incident analysis. Digital forensics is a branch of Forensic Science that focuses on the recovery and investigation of material found on digital devices in connection with cybercrime [5]. Digital forensics can thus be defined as a process aimed at identifying, obtaining, preserving and analysing electronic evidence, while ensuring that it remains consistent and that its use complies with legal norms. For digital evidence to be admissible in a court of law, it must meet a number of criteria, including authenticity, which means it reflects its original form; integrity, which ensures that any changes made can be tracked; compliance, which guarantees the importance of the evidence in a particular case; and permissibility, which determines that it has been obtained in accordance with the law.

Digital forensics employs a range of methods to ensure that these criteria are met, with disk imaging being of particular significance. This process involves the creation of an exact copy of the contents of a digital device using tools such as FTC Imager and dd. The process of data extraction allows for the retrieval of information from devices, including the restoration of deleted files. The analysis of network data using tools like Wireshark facilitates the identification of crucial evidence. Additionally, analysis of the file system and metadata is performed to determine the origin, change history, and other relevant details of documents and other electronic files.

Cryptographic methods, including hash functions such as MD5 and SHA-256, are also used to ensure the consistency and authenticity of electronic evidence, which allows one to check if data has been altered after it has been acquired. Digital signatures are used to authenticate documents and emails. Furthermore, the exploration of

communications and social networks, encompassing email and messaging analysis, the restoration of deleted posts, and the acquisition of information from social networks using open-source intelligence (OSINT) methods, is of paramount importance. The employment of OSINT methods facilitates the systematic search and analysis of identity-related information available on the Internet, thereby aiding in the identification of potential attack vectors and the implementation of preventive measures [23].

The utilisation of artificial intelligence has become increasingly pivotal in contemporary society, as automated data analysis methodologies facilitate the expeditious and precise identification of significant trends and anomalies. Artificial intelligence algorithms find application in domains such as facial and object recognition, a field of particular importance in the realm of digital forensics, encompassing image and video material.

A plethora of standards have been developed to ensure the security of data. Notable among these are: 1) Global Guidelines for Digital Forensics laboratories [15], which offers detailed guidelines for the establishment and operation of digital forensic laboratories covering topics such as staff qualifications, ethical standards, laboratory infrastructure and quality control procedures. The objective is to assist laboratories globally in developing standardised procedures for the procurement and examination of digital evidence that is admissible in court; 2) Best Practice Manual for the Forensic Examination of Digital Technology [9]. This manual provides guidance on best practices for the forensic examination of digital technologies. It includes guidelines on the taking, analysis and preservation of evidence and stresses the need for standardised methods and procedures to ensure the integrity and credibility of evidence in judicial proceedings; 3) the ISO/IEC STANDARD 21037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence [14] is a set of guidelines for the identification, collection, acquisition and preservation of digital evidence. The purpose of the Standard is to assist organisations and professionals in ensuring that digital evidence is processed in accordance with internationally accepted standards, thereby preserving its integrity and admissibility in a court of law.

Adherence to these documents is imperative for ensuring the processing of digital evidence is conducted professionally and in accordance with international standards, thereby contributing to the credibility and efficiency of the judicial process.

Notwithstanding the advancements in digital forensics, numerous challenges persist in guaranteeing the credibility of electronic evidence. A salient issue is the rapid evolution of technology, necessitating the development of novel analytical tools and methods. Jurisdictional challenges further complicate the acquisition of evidence, as it frequently falls outside the scope of national legal control. Scientific literature indicates potential issues in data interpretation. For example, a study conducted by Itiel Dror and Nina Sunde found that experts' observations can be

influenced by the contextual information provided to them and that consistency between expert analyses is often low. The authors emphasized the need for quality assurance measures to mitigate these biases and improve the reliability of the digital forensics' process [6].

In order to enhance the credibility of digital evidence, it is imperative to harmonise legislation to circumvent interpretative ambiguities and divergent approaches across jurisdictions. However, it is crucial to acknowledge that the admissibility, relevance and reliability of the evidence, as well as the burden of proof, rests with the national legal systems concerned. The European Court of Human Rights [7] has repeatedly emphasised that it does not function as the fourth body to examine the rules on admissibility and exclusion of evidence.

The new legal instruments, namely (1) Regulation (EU) 2023/1543, which provides a legal framework under which a Member State authority may require a service provider operating in the EU to provide or retain electronic evidence, irrespective of the location of the data, European Union, 2023/1543, (applies from 18 August 2026); and (2) Directive (EU) 2023/1544 laying down rules on the appointment of specially designated authorities and legal representatives to service providers offering services in EU. These designated authorities are entrusted with the responsibility of adopting, enforcing and implementing orders pertaining to the procurement of electronic evidence within the context of criminal proceedings (European Union, 2023/1544). This directive had to be incorporated into the national legal frameworks by 18 February 2026. However, it is noteworthy that these authorities do not regulate the admissibility of evidence at the national level. The determination of admissibility of evidence rests exclusively with the national provisions of EU law, rather than those of European Union law.

The electronic evidence regulation is principally focused on facilitating more efficient and expeditious access to electronic evidence. This is based on the assumption of mutual trust between EU Member States and the presumption that fundamental rights are adequately protected. However, in practice, this trust is not always justified, particularly due to concerns regarding the rule of law in certain states, meaning that the existing safeguards may be insufficient. In circumstances where such trust is lacking, it is essential to implement stronger protections for fundamental rights, as emphasized in Shurson's article [24].

The introduction of new technologies capable of more effectively analyzing and authenticating electronic evidence is also essential. International cooperation is of critical importance, as digital evidence is frequently stored across different legal jurisdictions, which can result in restricted access to that evidence. Digital forensics is an evolving field whose importance continues to grow due to the increasing integration of technology into both everyday life and legal processes. Consequently, in the future, there may be a necessity for more extensive deliberations on establishing uniform admissibility criteria at the European

Union level as a whole. This perspective is also endorsed by G. Lasagni [25].

In conclusion, this chapter suggests that the development of the legal framework on electronic evidence within the European Union reflects a continuing balance between improving the efficiency of criminal proceedings and safeguarding fundamental rights. Despite the fact that the newly developed legal instruments have been demonstrated to enhance cross-border access to electronic evidence, questions of admissibility remain largely within the jurisdiction of national legal systems. This has the potential to result in divergent approaches in practice. In this context, greater coherence in evidentiary standards and procedural safeguards may become an important topic for future discussion in order to strengthen legal certainty and the effective protection of rights across the European Union.

IV. CONCLUSIONS

The utilization of electronic evidence in legal proceedings holds considerable promise for enhancing the efficiency and effectiveness of justice in the digital era. At the same time, it reveals a range of structural, legal and technical challenges arising from the interaction between rapidly evolving technologies and existing legal frameworks. This article has examined the current regulation of electronic evidence, its degree of alignment with technological realities, and the principal difficulties encountered in practice. These include issues related to mutual trust between Member States, divergences in national approaches, technical challenges concerning the collection, preservation, authentication and interoperability of electronic evidence, as well as legal and procedural constraints linked to jurisdiction, data protection requirements and the safeguarding of fundamental rights. Collectively, these challenges affect legal certainty, procedural efficiency and the consistent application of justice across the European Union.

Future developments may therefore require a more coherent and technologically informed approach to electronic evidence, combining legal harmonization with enhanced technical capabilities. This includes the adoption of tools capable of ensuring the authenticity, integrity and traceability of digital data, alongside greater interoperability between competent authorities. Given the inherently cross-border nature of electronic evidence, stronger cooperation at both the EU and international levels remains essential. The continued evolution of this field will likely depend on the ability to reconcile technological developments with effective procedural safeguards and a more uniform protection of fundamental rights throughout the European legal order.

While recent EU instruments seek to facilitate cross-border access to electronic evidence and improve procedural cooperation, their effectiveness continues to rely significantly on the principle of mutual trust between Member States. However, practical experience demonstrates that mutual trust cannot always be presumed,

particularly in the context of ongoing concerns regarding the rule of law in certain jurisdictions. Consequently, the successful functioning of the electronic evidence framework depends not only on legislative harmonization at the EU level but also on the consistent implementation and enforcement of procedural safeguards at the national level, ensuring the effective and uniform application of common standards across Member States.

REFERENCES

- [1] J. Balodis-Bolužs, "Elektroniskā pierādījuma identitātes saturiskais definējums," *Juridiskā zinātne*, vol. 77, pp. 13–25, 2019. [Online]. Available: <https://doi.org/10.22364/juzk.77.13>.
- [2] V. Bukovskis, *Civilprocesa mācības grāmata*, Rīga: autora izdevums, 1933.
- [3] Civilprocesa likums, Latvijas Republikas likums, Latvijas Vēstnesis, 326/330, 03.11.1998. [Online]. Available: <https://likumi.lv/ta/id/50500-civilprocesa-likums>.
- [4] Court of Justice of the European Union, "Judgment in Case C-670/22, M.N. (EncroChat)," ECLI:EU:C:2024:3723, 2024, April 30.
- [5] EC-Council, "What is digital forensics?," EC-Council. [Online]. Available: [What is Digital Forensics In Cybersecurity? Phases, Careers & Tools](#).
- [6] I. Dror & N. Sunde, "A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making," *Forensic Science International: Digital Investigation*, vol. 36, pp. 200-210, 2021. [Online]. Available: [A hierarchy of expert performance \(HEP\) applied to digital forensics: Reliability and biasability in digital forensics decision making - ScienceDirect](#).
- [7] Elektronisko dokumentu likums, Latvijas Republikas likums, Latvijas Vēstnesis, 169, 20.11.2002. [Online]. Available: [Elektronisko dokumentu likums](#).
- [8] European Court of Human Rights, "Khan v. the United Kingdom [Judgment]," European Court of Human Rights, February, 2014.
- [9] European Network of Forensic Science Institutes (ENFSI), *Best practice manual for the forensic examination of digital technology*, ENFSI, January 24, 2024.
- [10] European Union, "Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for gathering electronic evidence in criminal proceedings," *Official Journal of the European Union*, 2023. [Online]. Available: [Directive - 2023/1544 - EN - EUR-Lex](#).
- [11] European Union, "Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings," *Official Journal of the European Union*, 2023. [Online]. Available: [Regulation - 2023/1543 - EN - EUR-Lex](#).
- [12] D. Gorgieva, E. Gjorgioska, & Z. Stoileva, "Electronic evidence in civil proceedings," *International Journal of Social Sciences and Humanities*, vol. 28, pp. 1-21, 2021. [Online]. Available: [ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS | Horizons - International Scientific Journal](#).
- [13] G. Horsman, "ACPO principles for digital evidence: Time for an update?," *Forensic Science International Reports*, vol. 100076, 2020. [Online]. Available: [ACPO principles for digital evidence: Time for an update? - ScienceDirect](#).
- [14] International Organization for Standardization/International Electrotechnical Commission, *ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*, ISO, 2012. [Online]. Available: [ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence](#).

- [15] INTERPOL, Global guidelines for digital forensics laboratories, INTERPOL, May 2019. [Online]. Available: https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf.
- [16] Kriminālprocesa likums, Latvijas Republikas likums, Latvijas Vēstnesis, 74, 11.05.2005. [Online]. Available: [Kriminālprocesa likums](#)
- [17] M. Krūmiņš, "Elektronisko pierādījumu vērtēšanas līkloči," Starptautisko un Eiropas Savienības tiesību piemērošana nacionālajās tiesās, pp. 312–318, 2020. [Online]. Available: [juzk.78.33-Krumins.pdf](#)
- [18] Latvijas Republikas Senāts, "Krimināllietu departamenta 2018. gada 22. augusta lēmums lietā Nr. 11250014115, SKK-297/2018," ECLI:LV:AT:2018:0822.11250014115.2.L, 2018.
- [19] M. K. Nickson, V. R. Kebande, H. S. Venter, & K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," Forensic Science International: Reports, vol. 1, 100008, 2019. [Online]. Available: [On the importance of standardising the process of generating digital forensic reports - ScienceDirect](#)
- [20] D. Ose, "Elektroniskā saziņa kā rakstveida pierādījums civilietā," Juridiskā zinātne, vol. 78, pp. 32-33, 2022. [Online]. Available: [juzk.78.03-Ose.pdf](#).
- [21] Pierādījums, Britannica. [Online]. Available: [Evidence | Definition, Law, Types, Examples, & Facts | Britannica](#)
- [22] Supreme Court of Norway, "HR-2019-610-A [Order]," Supreme Court of Norway, 2019. [Online]. Available: [hr-2019-610-a.pdf](#)
- [23] M. Walkow, & D. Pöhn, "Systematically searching for identity-related information in the internet with OSINT tools," arXiv preprint, arXiv:2407.16251, 2024. [Online]. Available: [\[2407.16251\] Systematically Searching for Identity-Related Information in the Internet with OSINT Tools](#)
- [24] J. Shurson, "The balance of efficiency and fundamental rights in the EU e-Evidence Regulation," New Journal of European Criminal Law, vol. 16, no. 3, 2025, doi: 10.1177/20322844251357090.
- [25] G. Lasagni, "Admissibility of digital evidence," in The Cambridge Handbook of Digital Evidence in Criminal Investigations, V. Franssen and S. Tosza, Eds., Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2025, pp. 126–152.

Cyber Threat Intelligence Based Scoping of Red Team Exercises

Svilen Kamdzhlov

IT Department

Nikola Vaptsarov Naval Academy

Varna, Bulgaria

s.kamdzhlov@naval-acad.bg

Dimitar Nikolov

IT Department

Nikola Vaptsarov Naval Academy

Varna, Bulgaria

d.nikolov@naval-acad.bg

Abstract – One of the most effective ways to test a company's security posture is through red team assessments and targeted penetration testing. This article defines one of the most effective approaches for determining the scope of the tests and the stages they go through. The stages include getting to understand the potential attackers, their tactics, techniques and procedures, the modus operandi and the objective with which they operate. The paper also discusses the importance of people, business processes, technology and distinguishing between important and critical assets as part of effective testing. It discusses the best tool for proper scoping is contextualized threat intelligence-based analysis and red team assessment frameworks such as TIBER-EU, CBEST and iCAST. This paper describes an approach that can be used to improve the scoping of the mentioned tests and hence increase their value.

Keywords – Asset classification, contextualized threat intelligence, penetration testing, red team assessments, threat modeling

I. INTRODUCTION

Over the past decade, cybersecurity assessments have evolved significantly - moving beyond traditional penetration testing toward more sophisticated, scenario-driven methodologies. While penetration testing focuses on identifying and confirming the exploitability of specific vulnerabilities, modern red team assessments evaluate an organization's broader security posture: its ability to detect, contain, and recover from realistic, targeted attacks. To meet this expanded mandate, disciplines such as adversary emulation, purple team exercises, and threat-informed red teaming have emerged, incorporating factors like social engineering, operational security, and situational awareness into the assessment model.

The red team concept originated [1] in Cold War-era military exercises, gaining large-scale adoption in the 1980s when the NSA pioneered its application in the intelligence community. The discipline entered the cyber domain following Mandiant's landmark 2013 APT1 report [2], which documented state-sponsored cyber espionage

campaigns and introduced the concept of Advanced Persistent Threats (APTs). This catalysed systematic TTP documentation efforts, culminating in the release of the MITRE ATT&CK [3] framework in 2015 - a comprehensive, community-driven knowledge base of adversary behaviours that has since become the common language of threat-informed defense. As APTs became better understood [4], regulated red team frameworks emerged to formalize assessment practices across the financial sector, including CBEST, TIBER-EU, iCAST, and others. While these frameworks affirm the central role of Cyber Threat Intelligence (CTI), they stop short of prescribing how assessments should be scoped and executed in practice - leaving a critical gap between high-level guidance and operational implementation.

The entry into force of the EU Cyber Resilience Act in December 2024, alongside updated NIST guidance, has sharpened a second, related gap: the near-exclusive focus of existing frameworks on financial institutions with conventional IT infrastructure. Critical infrastructure sectors - including power grids, industrial control systems, ports, and maritime assets - face comparable and in some cases greater APT exposure, yet no structured red team assessment framework governs their evaluation. While OT red teaming is described in practitioner literature, replicable methodologies for scoping and executing adversary emulation exercises in ICS, SCADA, and OT environments remain absent.

This paper addresses both gaps. Its primary focus is on defining penetration testing and red team assessment scope using CTI as the foundational input - a step that is underprescribed in existing frameworks yet disproportionately consequential for assessment quality. The intelligence cycle, threat actor profiling, TTP mapping, and asset contextualization are each examined in turn, and a worked example using a fictitious defense supply chain company is provided to illustrate how a complete, credible, and operationally relevant scope is constructed from first principles. The same approach is equally applicable to

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.210>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

penetration test scoping and to environments beyond the financial sector, including those dependent on operational technology.

II. RED TEAM ASSESSMENT FRAMEWORKS

One of the most common situations on the customer's side is the lack of understanding of the above mentioned approaches and the overall organization and execution of a Red Team assessment. Since many financial and political institutions have been in this position and guidance was definitely needed, several frameworks were developed. A not definitive list would include:

- CBEST Intelligence Led Testing, created by the Bank of England .
- Threat Intelligence-Based Ethical Red Teaming – TIBER-EU [6] (EU Red Team Assessment framework).
- Red Team: Adversarial Attack Simulation Exercises (AASE) – created and adhered to by the Association of Banks of Singapore [7].
- Intelligence-led Cyber Attack Simulation Testing (iCAST) – HKMA (the Hong Kong Monetary Authority adversary emulation exercise framework)
- G-7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT) [9].
- GFMA (Global Financial Markets Association) – a framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry.
- Intelligence-led Cyber Resilience Testing (I-CRT) Framework

A deeper look into the above listed frameworks shows that all of them consider threat intelligence based scope, fundamental to the assessment.

CBEST is a framework to deliver controlled, intelligence-led cybersecurity tests. The tests replicate the threat actors TTP's, considered by the UK Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions[10]. Institutions that are part of the United Kingdom's Financial Services Sector must remain resilient to cyber attack. To help these organizations achieve this, CBEST security assessment framework was implemented. CBEST proposes an intelligence-led penetration testing approach that replicates the actions of a cyber attacker's intent on compromising an organization's Critical Functions and the technology assets and people supporting those functions. Collaboration, evidence and improvement lie at the heart of CBEST [5] as well as a close liaison with the Bank of England and relevant regulators. For those organizations that form part of the Critical National Infrastructure liaison with GCHQ may also be required. The most specific feature of CBEST is its intelligence-led approach. The assessment process consists of four phases of work:

- Initiation Phase assessment: is formally launched, the scope is established, and TI/PT service providers are procured.

- Threat Intelligence Phase: the core threat intelligence deliverables are produced, threat scenarios are developed into a draft Penetration Test Plan, threat intelligence is assessed, and handed over to the PT provider.

- Penetration Testing Phase: an intelligence-led penetration test is planned, executed and reviewed, and detection and response capabilities are assessed.

- Closure Phase: Intelligence, Detection, and Response Report and Remediation Plan are finalized.

During the Threat Intelligence Phase and Penetration Testing Phase, the CBEST assessment is led by the TI service provider and PT service provider respectively.

TIBER-EU is a framework that delivers an intelligence-led red team PT. Intelligence-led red team assessments replicate the TTP's of real threat actors who, on the basis of threat intelligence analysis, are considered a genuine threat. An intelligence-led red team penetration test/red team assessment involves the use of a variety of techniques to simulate a complex attack on people, processes and technologies and measure the effectiveness of the client detection and response capabilities. The Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework enables EU authorities to build a program to test and improve the EU financial institutions resilience against sophisticated cyber attacks.

TIBER-EU is designed to be adopted by the relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool.

Hong Kong Monetary Authority (HKMA) has developed a Cyber Fortification Initiative (CFI), which comprises three components [8]:

- Cyber Resilience Assessment Framework (C-RAF)
- Cyber Intelligence Sharing Platform
- Professional Development Program(PDP)

C-RAF compromised the following elements:

- Inherent risk assessment
- Maturity assessment
- Intelligence-led cyber attack simulation testing (iCAST)

Under iCAST, the traditional penetration test is augmented by taking in consideration the knowledge of the penetration test provider and the relevant threat intelligence to build end-to-end testing scenarios (from attack initiation to achieving pre-defined test goals.

All of the mentioned frameworks' practical efficiency depends on cyber threat intelligence [11] and stress the importance and benefits of proper threat intelligence analysis. Unfortunately, the analysis and its results are often generalized and taken out of context.

The cyber threat intelligence lifecycle consists [12], in general, of five stages. It is a process model and has the

purpose of systematically collecting, processing and analyzing data in order to answer specific questions. The five stages are as follows:

1. Planning and direction
2. Collection
3. Analysis
4. Production
5. Dissemination and Feedback

Due to improper implementation of some of the phases or in some cases even breaking the Cyber Threat Intelligence Cycle, the result and correspondingly the scope are suboptimal and lead to suboptimal results.

Many of the customers lack or have inefficient Threat Intelligence programs and are unable to define the specific APT's and the campaigns relative to their geopolitical and industry context, technology and infrastructure. Due to that fact it is in general left to the assessor to decide what TTP's (Techniques, Tactics and Procedures) are relevant to the case and how to apply them, but the assessor usually does not have the resource to do a proper profiling of the target and select the most relevant TTP's, nor does he have the needed deep understanding of the business processes and priorities of the client. The CTIC [13] can and should be used in all steps of the definition and refinement of the engagement scope. The first step is to define the geopolitical and industry context of the client. Here a helpful approach for data collection is the interview of the client c-level supplemented by OSINT research. Regarding analysis techniques, some geopolitical and network analysis is a good starting point [14].

Once the industry and business network context are clear, the next step is to analyze the infrastructure and technological stack of the client. The data collection will be related again to document analysis of the provided diagrams and asset management data, and OSINT interpolation in order to understand the technological information readily available to the projected adversary. More than one CTIC [15] iteration might be needed in order to pinpoint the vital parts of the infrastructure.

Once the business and technology analysis of the client are concluded, the resulting product should form the base for the next stages related to the profiling of the potential adversary.

The first step of that stage is the search for threat actors and threat groups (TATG) with a history of attacks on businesses with similar business profile and geopolitical relations to the customer. Analysis should be mainly concentrated on episodes and campaigns in the last 2 years.

In the next step a technical analysis is to be executed, comparing the techniques, tactics and procedures (TTP's) of the potential TATG [16] and the infrastructure and technological stack of the customer. The product should define the relevant and applicable TTP's that could be included in the scope of the assessment.

The steps described above are also used by real threats, although with some differences in the methods and sources. In certain cases the APT's develop their target profile sometimes for over a year before the attack [17].

III. THE CTI LIFECYCLE AND ITS ROLE IN SCOPE DEFINITION

The following case study illustrates the practical application of adversary emulation methodology through a fictitious company designated SAT-SOFT, a Taiwan-based manufacturer of satellite hardware components and firmware whose business partners include direct suppliers to the U.S. Department of Defence Strategic Satellite Program. The company operates two production facilities with a third under construction, each site hosting a small office connected through a VPN to the main headquarters in Taipei. The on-premises network infrastructure consists primarily of Cisco and Netgear routers, Fortinet firewall devices, Windows workstations, at least one NAS server, and an Active Directory environment spanning multiple domains - a technological profile that closely mirrors the target architecture documented in Volt Typhoon operational reporting.

Following a threat profile analysis conducted by the Red Team Assessment Provider (RTAP)[18], the chosen Adversary Emulation Candidate was identified as the actor tracked by Microsoft as Volt Typhoon[19], by CrowdStrike as Vanguard Panda, by Palo Alto Networks Unit 42 as Insidious Taurus, and within the MITRE ATT&CK [20] framework as Bronze Silhouette. The selection was driven by the direct correspondence between the client's infrastructure - SOHO network[21] devices, Fortinet perimeter equipment, Active Directory[22], and supply chain relationships with defence contractors - and the documented targeting preferences and technical capabilities of the emulated threat actor. Mapping the actor's tactics, techniques, and procedures to the MITRE ATT&CK framework established a common operational language for all participating parties and formed the basis for scenario design across four assessment phases.

The first phase, Resource Development and Initial Access, targeted externally facing services and applications, with phishing campaigns and supply chain attack vectors directed at the new construction site incorporated to replicate the actor's known initial access methodology. At this stage the emulation replicates the actor's use of compromised SOHO devices - including Cisco, Netgear, ASUS, D-Link, and Zyxel routers - as command and control relay nodes, alongside deployment of custom Fast Reverse Proxy (FRP) clients with hardcoded C2 callbacks and port forwarding configurations established through native Netsh commands. Where phase one objectives were not achieved within defined parameters, the white cell - the controlling and coordinating authority of the exercise - retained authority to introduce assumed breach conditions to preserve assessment continuity.

The second phase, Lateral Movement, Privilege Escalation, and Persistence, proceeded on an assumed breach basis and focused exclusively on native tooling and

hands-on keyboard activity to replicate the actor's operational tradecraft as precisely as possible. The primary objectives were the acquisition of highly privileged Active Directory credentials, extraction of the ntds.dit file and SYSTEM registry hive through NTDSutil, and the establishment of durable persistence within the domain environment while maintaining the minimal forensic footprint characteristic of the emulated actor. The third phase, Discovery, directed operators to enumerate network topology, identify operational technology components including SCADA, HMI, and PLC systems where present, and map defensive capabilities including antivirus, EDR, and HIDS solutions using PowerShell, WMIC, and standard Windows command-line utilities consistent with the actor's documented discovery procedures. The fourth and final phase, Collection, Defence Evasion, and Exfiltration, targeted the acquisition of business-valuable data, industrial secrets, financial credentials, and non-destructive proof of control over operational technology systems, with operators required to maintain a low profile throughout and to employ the full range of Living-off-the-Land binaries - including certutil, lldifde, makecab, wevtutil, and impacket - to avoid detection and remove operational artefacts prior to withdrawal.

The primary deliverables of the assessment consisted of a comprehensive technical report and a structured debrief session conducted jointly with the blue team. The report, calibrated to its intended audience, documented targets achieved, successful and failed attack attempts, effective and failed defensive countermeasures, and a complete account of commands executed and their results. The debrief session served the dual purpose of exposing shortcomings in the defensive posture with actionable remediation guidance, and formally acknowledging the defensive activities that demonstrated the organisation's established level of cyber resilience - providing the client's business partners with the documented evidence of security maturity they had requested as a condition of continued supply chain participation.

IV. CONCLUSION

The definition of scope in red team and adversary emulation assessments is not a procedural formality - it is the foundational analytical act upon which the validity and operational relevance of the entire assessment depends. As this paper has demonstrated, a scope constructed without rigorous threat intelligence integration, without systematic application of the intelligence cycle, and without direct correspondence to the client's geopolitical exposure, technological profile, and business relationships will produce results that are technically competent but strategically meaningless. The SAT-SOFT case study illustrates the alternative: when threat profiling drives adversary selection, when the chosen Adversary Emulation Candidate's documented tactics, techniques, and procedures are mapped precisely to the client's infrastructure, and when assessment phases are structured to replicate the actual *modus operandi* of the most plausible threat actor, the outcomes of the exercise carry genuine predictive and defensive value. The intelligence cycle is not a preliminary step to be completed before the assessment

begins - it is a continuous analytical discipline that must be applied iteratively across every phase of scope definition, refinement, and execution.

The frameworks examined in this paper - whether grounded in MITRE ATT&CK, the Cyber Kill Chain, or structured red team methodologies - converge on a single operational principle: that the quality of an adversary emulation assessment is determined not by the sophistication of the tools deployed but by the fidelity with which the emulated threat reflects the adversary most likely to target the specific organisation under assessment. Clearly defined objectives, measurable targets at each assessment phase, and rigorous documentation of both successful and failed attack and defence activities are the instruments through which this fidelity is verified and communicated. As the threat landscape continues to evolve - and as state-sponsored actors such as Volt Typhoon demonstrate an increasing willingness to conduct long-duration, low-visibility operations against organisations that have never considered themselves high-value targets - the capacity to construct and execute intelligence-driven, threat-relevant assessments will determine whether organisations discover their vulnerabilities before their adversaries exploit them, or after.

ACKNOWLEDGEMENT

This research paper has received funding from Ministry of Education and Science of the Republic of Bulgaria under the National Science Program "SECURITY AND DEFENCE", in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No: 731/21.10.2021 and according to Agreement No: D01-74/19.05.2022.

REFERENCES

- [1] TechRound, "History of Red Team Exercises." [Online]. Available: <https://techround.co.uk/guides/history-red-team-exercises/> [Accessed: March 23, 2026].
- [2] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2021. [Online]. Available: <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf> [Accessed: March. 23, 2026].
- [3] MITRE ATT&CK, "ATT&CK Framework." [Online]. Available: <https://attack.mitre.org/> [Accessed: March 26, 2026].
- [4] Fortinet, "Red Team Assessment Solution Guide." [Online]. Available: <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-red-team-assessment.pdf> [Accessed: March 22, 2026].
- [5] CREST, "CBEST Framework." [Online]. Available: <https://www.crest-approved.org/membership/cbest/> [Accessed: March 23, 2026].
- [6] European Central Bank, "TIBER-EU Red Team Test Plan Guidance," 2025. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_red_team_test_plan_guidance_2025.en.pdf [Accessed: March 26, 2026].
- [7] Association of Banks in Singapore, "Red Team: Adversarial Attack Simulation Exercises Guidelines." [Online]. Available: <https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1->

- [06766a69f299c69658b7dff0006ed795.pdf](#) [Accessed: March 25, 2026].
- [8] Hong Kong Monetary Authority, "Intelligence-Led Cyber Attack Simulation Testing (iCAST)." [Online]. Available: <https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf> [Accessed: March 28, 2026].
- [9] G7, "Fundamental Elements for Threat-Led Penetration Testing," 2018. [Online]. Available: https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2018-G7-fundamental-elements-for-threat-led-penetration-testing.en.pdf [Accessed: March 26, 2026].
- [10] Global Financial Markets Association, "Threat-Led Penetration Testing Guidance." [Online]. Available: <https://www.gfma.org/wp-content/uploads/0/83/197/231/fff190cf-305a-44a6-a429-39848f22a48b.pdf> [Accessed: March 28, 2026].
- [11] Z. Wang, O. D. Adeyemo and E. A. Akinsoto, "Summary of Cyber Threat Intelligence," Int. J. Innov. Res. Multidiscip. Field, Vol. 8, № 3, Mar. 2022. [Online]. Available: <https://www.ijirmf.com/wp-content/uploads/IJIRMF202203006.pdf> [Accessed: March 28, 2026].
- [12] R. Brown and R. M. Lee, "The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey," SANS Institute, 2019. [Online]. Available: <https://www.sans.org/white-papers/38790/> [Accessed: Apr. 02, 2026].
- [13] Google Cloud, "Hands-On Introduction to Mandiant Approach to OT Red Teaming." [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/hands-on-introduction-to-mandiant-approach-to-ot-red-teaming> [Accessed: Apr. 02, 2026].
- [14] SANS Institute, "ICS Cyber Kill Chain." [Online]. Available: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf [Accessed: Apr. 02, 2026].
- [15] Cybersecurity and Infrastructure Security Agency, "Red Team Assessment Reveals Key Cybersecurity Gaps in Critical Infrastructure Organization." [Online]. Available: <https://industrialcyber.co/cisa/cisa-red-team-assessment-reveals-key-cybersecurity-gaps-in-critical-infrastructure-organization/> [Accessed: March 28, 2026].
- [16] MITRE, "APT3 Adversary Emulation Plan." [Online]. Available: https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf [Accessed: March 30, 2026].
- [17] Hong Kong Monetary Authority, "Cyber Resilience Assessment Framework (C-RAF)," 2016. [Online]. Available: https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA%20CFI%20-%20Cyber%20Resilience%20Assessment%20Framework%20-%20Dec%202016.pdf [Accessed: Apr. 02, 2026].
- [18] MITRE ATT&CK, "APT Group G1017." [Online]. Available: <https://attack.mitre.org/groups/G1017/> [Accessed: Apr. 02, 2026].
- [19] D. Dimitrov and E. Andreev, "China's Strategic Competition in Cyberspace: Volt Typhoon and Salt Typhoon as a Projection of Power, a More Aggressive Posture and a Future Beyond Espionage," Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, vol. 2, pp. 115-122, 2025. Available: <https://doi.org/10.17770/etr2025vol2.8618> [Accessed: March 26, 2026].
- [20] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Advisory AA24-038A." [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> [Accessed Apr. 04, 2026].
- [21] Office of the Superintendent of Financial Institutions, "Intelligence-Led Cyber Resilience Testing (I-CRT) Framework." [Online]. Available: <https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfis-intelligence-led-cyber-resilience-testing-crt-framework> [Accessed: Apr. 04, 2026].
- [22] NVISO Labs, "Attack and Defense in OT: Enhancing Cyber Resilience in Industrial Systems with Red Team Operations," Feb. 28, 2025. [Online]. Available: <https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfis-intelligence-led-cyber-resilience-testing-crt-framework> [Accessed Apr. 02, 2026].

Human Capital Development in War and Post-War Times Using Artificial Intelligence

Svitlana Kizim

Department of Digital Technologies
and Vocational Education Vinnytsia
Mykhailo Kotsiubynskyi State
Pedagogical University
Vinnytsia, Ukraine
skizim2012@gmail.com

Oksana Voloshyna

Department of Pedagogy and
Educational Management
Vinnytsia Mykhailo Kotsiubynskyi
State Pedagogical University
Vinnytsia, Ukraine
woloshina5555@gmail.com

Liudmyla Bondarchuk

Department of Management and
Administration Vinnytsia Institute of
Trade and Economics of State
University of Trade and Economics
Vinnytsia Ukraine
l.bondarchuk@vtei.edu.ua

Svitlana Nahorniak

Department of Pedagogy and
Educational Management
Vinnytsia Mykhailo Kotsiubynskyi
State Pedagogical University
Vinnytsia, Ukraine
svitlanamagor@gmail.com

Olena Stoliarenko

Department of Pedagogy and
Educational Management
Vinnytsia Mykhailo Kotsiubynskyi
State Pedagogical University
Vinnytsia, Ukraine
olena-best@ukr.net

Abstract—This paper examines human capital development in wartime and post-war recovery using artificial intelligence technologies as a key engineering instrument of transformation. Human capital is considered as a multidimensional system that includes vital, intellectual, social, and digital components, all of which have undergone significant changes due to demographic losses, forced migration, destruction of educational infrastructure, and labour market imbalances.

The methodological framework of the study is based on an interdisciplinary approach combining system analysis, conceptual modelling, statistical data analysis, and predictive modelling. This approach enables the identification of key risks of human capital degradation and substantiates the need for a transition to data-driven and engineering-oriented management.

It is demonstrated that artificial intelligence acts as a system-forming factor in human capital development by ensuring personalized learning, continuity of education, adaptive learning environments, and effective alignment with labour market demands. The study proposes an engineering architecture that integrates data-driven management, adaptive learning systems, virtual simulation environments, and digital platforms.

The scientific novelty of the research lies in the development of a roadmap for post-war human capital recovery based on the principles of engineering design and data-driven management. The proposed model defines a sequence of stages from stabilization of vital capital to long-term sustainability, ensuring coordinated recovery of all structural components. Practical implementation includes the use of generative models, adaptive educational platforms,

and labour market analytics systems to create individualized learning trajectories and improve the efficiency of human resource utilization.

It is concluded that artificial intelligence serves as a fundamental driver of human capital development in wartime and post-war conditions, enabling accelerated economic recovery, increased competitiveness, and the formation of a knowledge-based, innovative economy.

Keywords: artificial intelligence, digital transformation, human capital, post war recovery, wartime conditions

I. INTRODUCTION

The full-scale Russian invasion of Ukraine in 2022 caused transformations in all domains of social life, especially in the formation and development of human capital. Demographic losses, forced migration, the decline in employment significantly affected quantitative and qualitative characteristics of human capital as the main strategic resource of the nation.

In this context, the integration of artificial intelligence (AI) technologies as a powerful instrument of preservation, recovery and augmentation of human potential acquires particular importance. AI is crucial for ensuring continuous learning amidst instability, personalized studying, automatized evaluation, and creation of adaptable learning environment.

The matter of the impact of war conflicts on human capital is a subject of active research in modern literature.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.188>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Gorodnichenko et al. in his analysis of war consequences for Ukraine determines that armed conflicts lead not only to demographic losses, but also to compromised quality of education, deterioration in population health, which has long-term negative influence on economic growth. Authors emphasise on the necessity of investments in the quality of school education, higher education, and lastly, the retraining system as key areas for the recovery of human capital [1].

Kruglov and Tereshchenko indicate that war substantially aggravates metrics of human capital due to reduced access to quality education, migration of pedagogical personnel, psychoemotional exhaustion of the educational process participants [2]. Similar conclusions are found in the work of Yeremenko, who regards retraining and lifelong learning as anti-crisis instruments of the intellectual capital preservation in a wartime setting [3].

Special attention in literature is dedicated to the role of digital technologies and artificial intelligence in surmounting the educational challenges of warfare. Ober analyses the evolution of ICT (information and communication technologies) and AI usage in Ukrainian education during COVID-19 pandemic as well as in the war state, proposing the model of implementation of technologies in crisis situations [4].

In the post-war rebuilding context, Kuranda considers artificial intelligence to be a factor of the convergence of labour and capital, capable of compensating the human resources deficit owing to enhanced productivity [5]. Smykovska directly defines AI as the instrument of human capital development in the post-war economy of Ukraine [6].

The purpose of this article is to provide a comprehensive analysis of the transformations in human capital development in Ukraine during wartime and the postwar recovery, as well as to develop a roadmap for the postwar restoration of human capital.

II. MATERIALS AND METHODS

The methodological foundation of this study is an interdisciplinary approach that integrates principles from human capital theory, pedagogy, labour economics, digital transformation, and systems analysis.

System analysis was used as the primary research method to examine human capital as a holistic system of interconnected elements. The application of this method made it possible to identify the interrelationships between the vital, intellectual, social, and digital components of human capital, as well as to reveal the complex impact of war-related factors on their development.

Structural-functional analysis was applied to identify the main components of human capital, determine their functions, and analyze the changes caused by military events. Content analysis of scientific publications, documents, and analytical reports was used to identify contemporary approaches to human capital development and opportunities for applying artificial intelligence in education, vocational training, employment, and social

integration. Statistical data analysis was used to assess the scale of human capital losses resulting from the war.

A foresight approach was used to identify promising areas for human capital development in the postwar period.

Conceptual modeling was used to develop an integrated model of the digital ecosystem for human capital development. The roadmapping method was used in the final stage of the study to develop a roadmap for the post-war restoration of Ukraine's human capital. Based on the results of systematic, statistical, comparative, and predictive analysis, a sequence of recovery stages was established, priority development areas were identified, artificial intelligence tools were selected, and the expected outcomes of their implementation were determined.

III. RESULTS AND DISCUSSION

Human capital within the scope of our research is examined as a multidimensional system, which integrates vital, intellectual, social and virtual (digital) components. Vital capital is associated with physical and psychoemotional state of the population health, intellectual – with levels of proficiency and competency, social – the quality of social relations and trust, virtual – digital skills; the ability to amalgamate into digital economics. The abovementioned structure allows to systematically assess losses and determine the instruments of their compensation. To be specific, for the development of vital capital, appropriate measure is the utilization of AI systems for psychoemotional state monitoring and early posttraumatic disorders diagnosis; in case of intellectual capital – the usage of adaptive educational platforms and language models; for social capital – analytics of social networks and recommender systems; in terms of virtual capital – digital educational ecosystems and apparatus for developing digital competencies.

TABLE 1 ANALYSIS OF THREATS TO HUMAN CAPITAL (QUANTITATIVE AND STRUCTURAL INDICATORS)

Capital constituent	Destructive factors and threats	Scale and systematic repercussions
Vital capital	Increase of disabilities, chronic post-traumatic disorder, decrease in income in 78% of population (Deloitte, 2023).	Critical decline in performance; the demand for AI-monitoring of psychoemotional state.
Intellectual capital	“Exodus of talent” (more than 14,5 million of migrants); destruction of educational infrastructure; loss of 5 million jobs.	Risk of long-term intellectual degradation; gaps in educational trajectories.
Social capital	Community disintegration (4,7 millions of internally displaced persons); destruction of connection; reduced trust in state universities.	Loss of social coordination; deficit of 4,5 million workers until 2032 [7].

War caused deep transformation of all components of human capital, which manifests in demographic losses, full-scale migration, destruction of educational

infrastructure, drop in employment. Artificial intelligence in this context is a systematic factor that enables the scaling of intellectual capabilities of humanity. Architectural engineering of decisions is grounded in creation of an integrated digital ecosystem that intertwines educational, economical, and social processes. The key element is data-driven management, realized via processing data of educational and social-economical registers with the usage of neural network models. This permits to forecast labour market needs, form individual educational trajectories, and detect early risks.

An essential element is adaptive learning environment, derived from machine learning algorithms, which provides personalization of the educational process in real time. Such systems modify content, tempo and difficulty of learning according to user's individual characteristics, which allows to markedly increase efficiency of staff training. Additional implemented features are virtual simulation complexes and VR/AR-technologies that construct safe conditions for forming professional skills in risky activity fields, among them medicine, engineering, military training.

Practical realization of aforesaid approaches anticipates generative models and digital education platforms. Modern models, such as ChatGPT, Google Gemini, Microsoft Copilot, perform functions of intellectual tutors, ensure generation of educational content, support academic work and analytical thinking development. Simultaneously into service have come platforms of quick retraining (Coursera, Duolingo), which facilitate the adaptation of population skills to dynamic needs of the labour market.

Utilization of AI for integration of veterans and internally displaced persons in economics plays a pivotal role. With respect to this, intellectual systems conduct an analysis of existing competencies, grant retraining recommendations and determine optimal professional trajectories. In addition, they might be used for psychoemotional state monitoring, a critically vital element for vital capital restoration.

In post-war period, the human capital recovery strategy should be rooted in unification of technological modernization and social adaptation. Priority objectives are creation of digital jobs, development of intellectual educational systems, implementation of labour market analytics in real time, creation of an innovational ecosystem.

We consider the following architecture:

- **Data-Driven Management:** deploying neural network models for processing Big Data in educational registers. It enables prediction of individual trajectories and performs preventive risk monitoring – from demotivation to poor academic performance [8].
- **Adaptive Modern Learning Environments (MLEs):** the architecture of MLEs is predicated on machine learning algorithms,

which modify content, tempo and difficulty of learning in real time. Systems operate with digital profiles of cognitive peculiarities and provide personalization at the microlearning level.

- **SMART-complexes and Virtual Simulators:** application of virtual learning complexes for modelling of professional situations in safe spaces [9]. It is fundamental for training of military experts, doctors and engineers, where there is no margin for error.
- **AI engineering ensures inclusion,** creates API-oriented interfaces for people with disabilities. In this system, teacher evolves into an architect of educational experience and facilitator, who operates on analyst data.

Modernization of staff training requires integration of generative models and platforms.

- **Generative LLM-models** (ChatGPT-4, Gemini, Copilot): used for academic writing support, automatized generation of educational content and personal AI-tutoring [10].
- **Adaptive reskilling platforms** (Coursera, Duolingo): function as tools for dynamic skills correction (Upskilling) in line with market queries.
- **Synergy of educational modes:** AI warrants merging of formal, non-formal and informal education through digital competencies registers [11].
- **Special emphasis is placed on economical adaptation of veterans and internally displaced persons.** AI systems permit the conduct of automated skill assessment for military personnel, establish optimal retraining in deficit areas in economics [7].

In our research, we propound the roadmap of post-war human capital restoration (Table 2). Its structure is based on the principles of engineering design and data-driven management. Sequence of stages matches the logic of systemic recovery, wherein each successive level builds on the outcomes of the preceding one.

TABLE 2. ROADMAP FOR POST-WAR HUMAN CAPITAL RECOVERY
 BASED ON AI ENGINEERING APPROACHES

Stage	Recovery Area	Primary Tasks	Engineering Decisions (AI)	Expected Outcomes
1	Recovery of vital capital	Health rehabilitation, support of psychoemotional state	AI-health monitoring, diagnostic systems, predictive health analytics	Growth of working capacity of the population, reduction in morbidity
2	Recovery of intellectual capital	Education modernization,	Adaptive learning systems,	Growth of quality of the education

		retraining / upskilling	LLM-models (ChatGPT, Google Gemini, Microsoft Copilot), learning analytics	
3	Recovery of social capital	Reintegration of internally displaced persons and veterans	AI-powered competence analysis systems, recommender systems, social analytics	Rise of social solidarity, unemployment decline
4	Development of digital (virtual) capital	Digital skills formation, access to technologies	EdTech-platforms (Coursera, Duolingo), cloud systems, digital ecosystems	Growth in digital literacy, development of innovation economics
5	Institutional integration and management	Politics and infrastructure formation	Big Data analytics, labour market forecasting, AI-driven decision systems	Labour market balance, effective human capital management
6	Long-term durability	Sustainability and innovations	Smart Cities, AI governance, cybersecurity systems, interoperable platforms	Enhancement of competitiveness and economic stability

A key element of the proposed architecture for post-war human capital recovery is not only the integration of artificial intelligence tools into education and the labor market, but also the establishment of a system for continuously monitoring the effectiveness of such interventions.

Within the proposed model, generative artificial intelligence systems serve as a form of intelligent feedback. They not only assess learning outcomes but also generate personalized recommendations for adjusting learning strategies, addressing skill gaps, and optimizing individual educational pathways. The integration of artificial intelligence into the educational process monitoring system facilitates the transition from retrospective assessment to predictive and adaptive human capital management.

Within the structure of the proposed digital ecosystem, monitoring serves as a central feedback loop that integrates educational analytics, the labor market, and social policy

Practical realization of the roadmap foresees widespread use of intellectual tools in educational sphere, labour market and social adaptability of the population. Utilization of generative models, namely ChatGPT, Google Gemini and Microsoft Copilot, renders personalized learning, automatized educational processes and digital

competencies development [12]. Concurrently, the application of lifelong learning platforms, such as Coursera and Duolingo, fosters quick retraining and population adaptability to labour market changes. Collectively, it forges an innovative ecosystem, able to provide effective human capital recovery and construct prerequisites for economical sustainability in post-war time.

IV. CONCLUSIONS

The post-war transformation should culminate in the formation of a national intellectual ecosystem. It stands for a holistic space that blends adaptive systems of learning management, digital platforms of labour market forecasting, integrity assurance services and registers of professional qualifications.

As for the role of artificial intelligence in this system, it acts as a fundamental instrument of modernization, which ensures flexibility, transparency and predictability of personality development. Systematic integration of intellectual technologies will enable the transformation of human capital of Ukraine into the most competitive asset in Europe. Post-war recovery should occur not as reversion to pre-reform state, but as an innovative leap into the future, wherein AI serves as a key constituent of social mobility and nation sustainability.

REFERENCES

- [1] Y. Gorodnichenko, M. Kudlyak, and A. Şahin, "The effect of the war on human capital in Ukraine and the path for rebuilding," IZA Institute of Labor Economics, IZA Policy Paper No. 185, Jun. 2022. [Online]. Available: <https://docs.iza.org/pp185.pdf>
- [2] V. V. Kruglov and D. A. Tereshchenko, "Derzhavna polityka vidnovlennia liudskoho kapitalu Ukrainy v pislivoiennnyi period (State policy of human capital recovery in Ukraine in the post-war period)," *Osvitnia analityka Ukrainy (Educational Analytics of Ukraine)*, no. 2, pp. 21–33, 2023. [Online]. Available: https://science.ica.gov.ua/wp-content/uploads/2023/07/2_Kruglov_Tereshchenko_223_2023_21-33.pdf
- [3] O. Yeremenko, "Retraining and lifelong learning as an anti-crisis tool: Preserving Ukraine's intellectual capital in times of war," *Knowledge Economy and Lifelong Learning*, vol. 2, no. 1, pp. 48–66, 2026, [https://doi.org/10.61093/kell.2\(1\).48-66.2026](https://doi.org/10.61093/kell.2(1).48-66.2026).
- [4] J. Ober, T. Matushevych, and O. Strutynska, "From challenges to opportunities: Using ICT and AI in Ukrainian education in times of pandemic and war," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 11, no. 4, p. 100639, 2025, <https://doi.org/10.1016/j.joitmc.2025.100639>.
- [5] M. V. Kuranda and O. A. Bohutska, "Artificial intelligence as a convergence factor between labor and capital: Potential applications for Ukraine's economic development," *Ekonomika promyslovosti (Economy of Industry)*, no. 3, 2025, <https://doi.org/10.15407/econindustry2025.02.041>.
- [6] Yu. O. Smykovska, "Shtuchnyi intelekt yak instrument dlia rozvytku liudskoho kapitalu (Artificial intelligence as a tool for human capital development)," in *Proc. Student Conf. "Current Issues of Development and Stabilization of Ukraine's Economy in Wartime"*, 2025. [Online]. Available: <https://ekmair.ukma.edu.ua/>
- [7] V. M. Luhova and B. P. Makov, "Vykorystannia liudskoho kapitalu u pislivoiennii vidbudovi Ukrainy (Use of human capital in post-war reconstruction of Ukraine)," *Ukrainian Journal of Applied Economics and Technology*, vol. 9, no. 4, pp. 46–50, 2024, <https://doi.org/10.36887/2415-8453-2024-4-7>.
- [8] A. M. Gurzhi and M. A. Prykhodii, "Shtuchnyi intelekt yak stratehichniy chynnyk rozvytku liudskoho kapitalu v umovakh tsyfrovoy transformatsii (Artificial intelligence as a strategic factor in human capital development in the context of digital

- transformation),” in Proc. XX All-Ukrainian Sci. Pract. Conf. “Scientific and Methodological Support of Vocational Education and Training”, Kyiv, Ukraine, 2025, pp. 71–78.
- [9] N. Y. Dmitrenko, O. V. Voloshyna, S. S. Kizim, K. V. Mnyshenko, and S. V. Nahorniak, “Smart education in the prospective teachers’ training,” CTE Workshop Proceedings, vol. 10, pp. 414–429, 2023, <https://doi.org/10.55056/cte.568>.
- [10] S. Kizim, O. Voloshyna, I. Sarancha, S. Nahorniak, and O. Stoliarenko, “Organization of adaptive training using artificial intelligence technologies in the context of war environment,” in Proc. 16th Int. Sci. Practical Conf. Environment. Technology. Resources, Rezekne, Latvia, 2025, pp. 205–212, <https://doi.org/10.17770/etr2025vol2.8606>.
- [11] A. Yarovy, A. Yarovy, S. Kizim, and V. Ozeranskyi, “Innovative trends in the field of modern artificial intelligence methodology,” Environment. Technology. Resources, vol. 2, pp. 132–137, Jun. 2024, <https://doi.org/10.17770/etr2024vol2.8065>.
- [12] O. Voloshyna, T. Melnychuk, M. Sapohov, N. Burlaka, and A. Khilya, “The potential of developing and creating online applications for teacher training,” in Proc. 15th Int. Sci. Practical Conf. Environment. Technology. Resources, Rezekne, Latvia, 2024, pp. 525–529, <https://doi.org/10.17770/etr2024vol2.8086>.

A Conceptual Model for Information Security Assessment in Judicial Information Systems Based on Risk and Regulatory Requirements

Nikolay Koev
University of Library Studies and
Information Technologies
Sofia, Bulgaria
4623497-2@unibit.bg

George Dimitrov
Faculty of Information Sciences,
Computer Sciences Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
g.g.dimitrov@unibit.bg

Daniela Pavlova
Faculty of Information Sciences,
Computer Sciences Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Nikolay Penev
University of Library Studies and
Information Technologies
Sofia, Bulgaria
4623496-2@unibit.bg

Abstract—The increasing digitalization of the judicial sector requires the implementation of complex information systems that ensure high levels of information security, especially when processing sensitive and classified data. However, the application of security requirements in such environments is often fragmented due to the complexity of regulatory frameworks and the lack of structured approaches for risk assessment. This paper proposes a conceptual model for information security assessment in judicial information systems based on risk and regulatory requirements. The model integrates fundamental principles of information security, including confidentiality, integrity, and availability, with applicable legal and organizational constraints. It provides a structured approach for identifying assets, assessing risks, ensuring compliance with regulatory standards, and selecting appropriate security measures. The proposed model is designed to support decision-making processes and improve the effectiveness of security implementation during the deployment of complex information systems in the judicial sector. The results demonstrate that the model enhances the consistency and traceability of security-related decisions and facilitates alignment with established security standards and legal requirements.

Keywords—information security, judicial information systems, regulatory requirements, risk assessment.

I. INTRODUCTION

The implementation of electronic justice in the Republic of Bulgaria began gradually in 2017, following

the entry into force of amendments to the Civil Procedure Code. Its practical deployment continued in the subsequent years, during which the Unified Information System of the Courts was also introduced. Electronic justice involves the use of information and communication technologies within the judicial system. The digitalization of judicial activities already encompasses electronic case files, electronic submission of documents, internal case management systems, electronic service of documents, videoconferencing hearings, and data exchange with other public authorities. In addition to paper-based case files, cases are now also maintained electronically; summonses and notifications are served electronically; parties can monitor their cases online through the Unified Portal for Electronic Justice; and they can submit and sign documents using electronic signatures. Research on the development of e-justice shows that these processes simultaneously affect access to justice, the efficiency of judicial administration, data protection, and the guarantees of a fair trial [1]-[5]. This dependence on digital infrastructure transforms information security into a strategic factor for the proper functioning of the judiciary.

The problem is not limited to the implementation of individual technical measures. Judicial information systems process personal data, procedural documents, metadata and logs related to the actions of participants, electronic signatures, and, in certain cases, classified information. At the same time, risk management practice in information security shows that courts, as organizational

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.120>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

units, operate with a high degree of institutional independence. They apply different security procedures and do not have a unified risk management instruction applicable to all courts. This has an adverse impact on the overall monitoring of risk and weakens the connection between the judicial system as a whole, its control mechanisms, and regulatory compliance [6], [7]. In this respect, prosecution offices are organized under the authority of the Prosecutor General and strictly follow the principle of subordination by implementing the instructions issued by the highest authority within the prosecution system.

International frameworks for risk management and information security provide well-developed principles for asset identification, impact analysis, risk treatment, and continual improvement [8]-[12]. However, for the judicial sector, these frameworks are not sufficient on their own, as they must be applied in an environment subject simultaneously to substantive legal, procedural, organizational, and technological constraints. Of particular importance are the rules concerning personal data protection, the protection of classified information, electronic identification, compliance with internal rules, and the statutory and subordinate legislative acts governing the activities of the judicial system [13]-[22].

This creates the research need for a model that does not treat risk assessment and regulatory compliance as separate procedures but as interrelated layers of the same decision-making process. The aim of this study is to propose a conceptual model for information security assessment in judicial information systems that identifies critical assets and processes, assesses risk in dimensions relevant to judicial activity, maps risk to applicable regulatory requirements, and supports the selection and prioritization of security measures. The proposed model provides a systematic approach to identifying assets and critical infrastructure, managing risk, ensuring compliance with applicable requirements, and maintaining traceability of actions for audit purposes. The scientific novelty of the approach lies in the integration of a risk layer and a regulatory layer into a single decision-making mechanism adapted to the judicial institutional environment [8]-[12], [13]-[22].

II. MATERIALS AND METHODS

The study is conceptual and applies a combined qualitative approach based on three groups of sources. The first group includes standards and frameworks for risk management and information security: NIST SP 800-39, NIST SP 800-30 Rev. 1, ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO 31000:2018, the NIST Cybersecurity Framework 2.0, and NIST SP 800-61 Rev. 3 [8]-[12], [23], [24]. The second group includes scientific publications on information security, risk assessment practices, and the digital transformation of courts [1]-[7], [25], [26]. The third group includes applicable European and national regulatory acts [13]-[22].

To improve the transparency and reproducibility of the conceptual procedure, the development of the model

followed a four-step analytical process. First, the relevant literature on e-justice, information security risk management, and cybersecurity in judicial systems was reviewed. Second, international standards and frameworks were examined in order to identify recurring risk management components, including asset identification, impact assessment, risk treatment, monitoring, and continual improvement. Third, applicable European and Bulgarian regulatory requirements were mapped to the identified security dimensions. Fourth, the resulting model was analytically applied to three representative judicial scenarios: electronic submission of procedural documents, administration of electronic case files, and storage, archiving, and destruction of judicial information after the expiry of statutory retention periods.

The scope of the model includes the information assets, processes, and resources in the judicial system that are related to the creation, processing, exchange, storage, and archiving of classified and other sensitive information. For the purposes of the model, assets are grouped into six classes: information assets; application and infrastructure assets; authentication instruments; evidentiary materials; organizational roles; and related external services. The conceptual model is based on the principles of confidentiality, integrity, and availability, supplemented by the principles of "need to know", defense in depth, and least privilege. For each class, security criteria are defined that extend the classical triad with three additional dimensions: authenticity, traceability, and legal admissibility. These dimensions are particularly important in the judicial environment, since the validity of electronic actions, the provability of procedural actions, and the reliability of digital evidence have direct procedural significance [10], [11], [15], [16], [18], [19], [21], [22], [26].

III. RESULTS AND DISCUSSION

A. Architecture of the Proposed Model

The proposed model contains six consecutive stages: defining the scope and management roles; identifying and classifying assets; assessing risk; mapping regulatory requirements; selecting and prioritizing security measures; and monitoring, incident response, and improvement of the risk strategy. Within this structure, risk assessment is directly linked to regulatory compliance and practical security management so that each decision can be justified technically, organizationally, and legally. This turns the model into an applicable decision-making framework for the judicial institutional environment [8], [9], [23], [24].

The first stage defines the scope of the assessment by describing the judicial process, information flows, participating roles, and dependencies on external systems. Instead of treating the system only as a software product, the model describes it as a sociotechnical environment in which judges, court clerks, system administrators, lawyers, citizens, external authorities, and suppliers interact. This approach follows observations in the literature on the digital transformation of courts, according to which the effect of technology depends not only on the implemented

platform but also on working practices, management mechanisms, and organizational acceptance [3]-[5].

The second stage introduces an asset-oriented view of the judicial information system. In practical terms, this means describing not only databases, networks, and applications, but also electronic case files, metadata related to procedural actions, participant identifiers, certificates, event logs, archives, backups, interfaces to registers, and repositories for electronic evidence. This approach helps avoid a common weakness in organizational practice, where risk assessment focuses primarily on infrastructure while underestimating the importance of security procedures, sensitive information, and evidentiary materials [6], [7].

The third stage is risk assessment. In the model, risk is determined through a combined assessment of probability, impact, and conditions of use. For the judicial environment, impact is examined across five dimensions: technological, procedural, substantive legal, organizational, and reputational. For example, the temporary unavailability of the Unified Portal for Electronic Justice may appear to be a technically limited incident, but in certain situations it may prevent the submission of a document and thus produce procedural and legal consequences, such as the preclusion of a party's right to submit a response within the statutory time limit. Similarly, a breach of integrity in the logs may not directly damage the main database, but it may compromise the evidentiary reliability of the actions performed. This extended assessment allows risk to be measured more closely in relation to the actual function of the judicial system, rather than solely according to general IT criteria [1], [2], [13], [16], [19], [22].

Table I summarizes the logic of the model by stages, key questions, and expected results. It shows that security assessment does not start from a checklist of controls but from the judicial function of the system and the type of assets that must be protected.

TABLE I. PHASES OF THE PROPOSED MODEL

Stage	Content and result
Scope and roles	Documentation of the process, the participants, the chronological and hierarchical sequence of activities, the roles of the participants involved, and the systems used.
Assets	Catalogue of information, technological, authentication, and evidentiary assets, including critical infrastructure.
Risk	Assessment of probability and impact in technological, procedural, legal, organizational, and reputational dimensions.
Regulatory mapping	Linking risk to applicable regulations, laws, ordinances, and internal rules.
Controls	Prioritization of technical, organizational, and procedural measures.
Monitoring	Indicators, incident readiness, audit, continuous monitoring of the process, and improvement.

The fourth stage is regulatory mapping. This is the main distinguishing feature of the proposed model. For each

identified risk, a set of applicable regulatory requirements and internal rules is identified, defining the minimum acceptable level of protection. When personal data are processed, this includes the rules of the GDPR (General Data Protection Regulation), the Personal Data Protection Act, and the national cybersecurity framework; for authentication and signing, it includes eIDAS (electronic identification and trust services regulation) and the internal rules of the judiciary; for electronic procedural actions, it includes Ordinance No. 6 on the performance of procedural actions and certifying statements in electronic form; and for classified information, it includes the Classified Information Protection Act, the Rules for Implementation of the Classified Information Protection Act, and the Ordinance on the Security of Communication and Information Systems [13]-[22]. Regulatory mapping does not replace legal analysis; rather, it structures it so that it can be operationally used in risk management.

The fifth stage covers the selection of security measures. Here, the model applies a combined logic. On the one hand, measures are selected according to the level of risk; on the other hand, they are checked against the mandatory minimum requirements arising from the regulatory framework. This avoids two extreme scenarios: formal implementation of a control without a link to the actual risk, and low-cost risk optimization that does not meet the regulatory minimum. The groups of measures include access management, cryptographic protection, segregation of roles, chronological ordering of logs, administration, data storage, archiving and recovery, accreditation, secure administration, training, and supplier oversight [10], [11], [17], [19], [23]-[26].

The sixth stage introduces monitoring and improvement. In this stage, the model is linked to the principles of CSF 2.0 (Cybersecurity Framework) and the incident response guidance in NIST SP 800-61 Rev. 3, requiring the tracking of indicators for access, data modifications, policy violations, failures of system components, and incidents in exchanges with external systems [23], [24]. For the judicial environment, it is particularly important that these indicators be linked to predefined impact scenarios, such as unsuccessful electronic service of documents, compromise of an electronic signature, unauthorized extraction of a case file, or breach of the chain of custody of digital evidence.

B. Risk - Regulatory Criticality Matrix

This sequence supports the traceability of decisions and makes it easier to justify them before management, an audit body, or an external supervisory authority.

To make the model applicable in practice, risk is assessed not only by combining probability and impact, but also by introducing a regulatory criticality coefficient. Regulatory criticality reflects the extent to which a given risk affects compliance with laws, regulations, and internal rules. It is expressed numerically and indicates how critical a given event is in relation to regulatory requirements. It includes conflicts with legislation, non-compliance with internal rules, prescriptions issued following inspections by

supervisory authorities, and obligations related to the protection of sensitive information. The formula used is:

$$\text{Risk} = \text{Probability} \times \text{Impact} \times \text{Regulatory Criticality} \quad (1)$$

This approach is particularly useful in the public sector, where the acceptability of risk cannot be determined solely by operational efficiency [8]-[12], [17]-[22].

In practice, the matrix uses three levels of regulatory criticality: basic, increased, and critical. Criticality is basic when it concerns general organizational requirements that do not directly affect procedural validity. Criticality is increased when it concerns requirements related to personal data, case administration, electronic identification, traceability, and accountability. Regulatory criticality is critical when it concerns classified information, digital evidence, accredited systems, or actions that may lead to challenges to procedural lawfulness. This step enables more realistic prioritization and reduces the risk of formally equal treatment of vulnerabilities that differ in legal significance.

Table II illustrates the way in which the model links typical judicial assets with regulatory focuses and groups of measures. What is important here is that the asset is not considered abstractly, but in relation to the process. For example, the electronic case file has a different protection profile from the system log, while the repository for digital evidence has a different protection profile from the public portal for inquiries. This differentiation is consistent with recent publications focused on cybersecurity in the judiciary and the protection of digital evidence [25], [26].

TABLE II. EXAMPLE MAPPING OF ASSETS, REGULATORY FOCUSES, AND MEASURES

Scenario	Regulatory focus and priority measures
Electronic submission	eIDAS, Ordinance No. 6, GDPR; strong identification, reliable administration, compliance with the statutory deadline, and confirmation of the statement.
Electronic case file	GDPR, Cybersecurity Act, Ordinance No. 1; role-based model, least privilege, confidentiality, integrity, and availability of information, and control of administrators.
Digital evidence and classified information	Classified Information Protection Act and the Ordinance on the Security of Communication and Information Systems; accreditation, cryptographic protection, compliance with the principles of "need to know" and "defense in depth", physical security, and personnel security.

C. Analytical Application of the Model

The first representative scenario is the electronic submission of documents and certifying statements. Here, the main risks are related to denial of authorship, unauthorized access, manipulation of the time of submission, incomplete documentation and administration,

and unavailability of access to the electronic case file at a critical moment concerning compliance with a statutory deadline. The regulatory focus falls on requirements for electronic identification, authentication of authorship, technical formats, logging of actions, and protection of personal data [13], [15], [21], [22]. In this scenario, the model leads to the priority introduction of strong identification, synchronized time, reliable administration, mechanisms for confirmation of the submitted statement, redundant access channels, and procedures for proving a technical incident.

The second scenario is the management of the electronic case file. Here, the main object of protection is not only the content of the case file but also its history: who created, read, edited, forwarded, or signed a specific document and under which access rights. It is also necessary to verify whether the "need-to-know" principle has been observed, namely whether access to certain data with a specific classification level was performed by a user whose level of authorization corresponds to that classification level and who acted in the performance of official duties or a specifically assigned task. The risks include unauthorized internal access, unlawful extraction of data sets, changes without trace and manipulation of information, system unavailability after updates, and insufficient separation of roles. In this scenario, the model emphasizes the need for a detailed rights model, minimization of privileges, strict control over administrative actions, immutable logs, and periodic checks of consistency between organizational roles and technically granted rights [10], [11], [17], [20], [23], [25].

The third scenario is the storage and processing of digital evidence and information under a special protection regime. This is precisely where classical IT criteria are most insufficient unless they are supplemented by requirements for authenticity, chain of custody, accreditation, and documentary provability. Publications on digital evidence in judicial information systems emphasize that protection must cover not only the medium but also the process of receiving, indexing, accessing, copying, analyzing, and presenting evidence before the court [26]. The Classified Information Protection Act and the Ordinance on the Security of Communication and Information Systems additionally impose specific organizational and technical measures, including accreditation, cryptographic security, physical security, document security, and personnel security, with the aim of ensuring the protection and control of responsible officials and system users [18], [19]. In this scenario, the proposed model provides the greatest benefit by linking technical controls with the evidentiary value of the processed information.

D. Discussion

The advantage of the proposed model is that it overcomes the traditional separation between a compliance checklist and risk assessment. This is important because, in the judicial environment, formal compliance with a given requirement does not automatically guarantee that the risk has been managed appropriately, and a low technical

assessment of a given risk does not mean that its legal consequences are insignificant. The combined approach enables more precise justification of priorities, better documentation of decisions, and clearer allocation of roles and responsibilities among technical teams, administrative management, security officers, and legal experts [6]-[9], [23]-[25].

The model also has organizational value. Research on e-justice shows that the real benefit of digitalization depends on institutional readiness and capacity for change, acceptance of the system by internal users, and the balance between efficiency and procedural guarantees [1]-[5]. When security decisions are traceable and well justified, both the acceptance of new procedures and internal control are facilitated. This is especially important when common platforms are implemented across many courts, where organizational differences in information security may lead to different levels of protection.

A limitation of the present study is that the model is conceptual and has not been validated through large-scale empirical application in multiple courts. It does not replace technical audits, penetration testing, digital forensics in the analysis of evidentiary materials, or an individual legal assessment of a specific case. Its purpose is to provide a structured framework that reduces fragmentation in decision-making and makes the relationship between asset, risk, regulatory requirement, and security measure clearer. Future research may develop the model through quantitative scales, profiles for different types of courts, and empirical comparison among implemented systems. A promising direction is also the inclusion of indicators for the quality and usability of judicial data, as recent research shows that data management is becoming key to assessing efficiency and fairness in justice [27].

E. Indicators for Subsequent Control

To be usable in an institutional environment, the model also includes a minimum set of indicators for subsequent control. They are grouped into four categories: indicators for access and identification; indicators for integrity and administration; indicators for continuity and recovery; and indicators for regulatory compliance. The first category includes failed login attempts, use of privileged accounts, deviations in user behavior, and actions outside the usual role. The second category includes changes to electronic case files, events without a digital signature or with a non-corresponding timestamp, and missing logs. The third category includes failures of critical services, time to detect an incident, time to recover, and the availability of verified backups. The fourth category includes deviations from internal policies, incomplete records of processing activities, lack of evidence of training, or gaps in accreditation documentation [13], [14], [17], [19], [23], [24].

The use of indicators should not be reduced to formal reporting. They are meaningful only when linked to specific management decisions: reconsidering roles and rights, reviewing access to classified case files and other sensitive information, updating incident response procedures, providing additional user training, or changing

the system architecture. From this perspective, the model functions as a cyclical mechanism for organizational learning rather than as a one-time assessment. Such a dynamic logic is consistent with risk management frameworks and the requirements of modern approaches to cybersecurity [8]-[12], [23], [24].

From a scientific perspective, this also enables better comparison among different judicial organizations. If assets, risks, regulatory focuses, and controls are described according to a unified scheme, it becomes possible to trace which problems recur most often, which measures have the strongest effect, and where the effective and improved organization of processes has the greatest impact on the level of security. In the long term, this opens the possibility of building sectoral profiles for judicial cybersecurity and empirically validating the model through comparable data from different institutions [7], [25], [27].

IV. CONCLUSIONS

The proposed conceptual model for information security assessment in judicial information systems integrates risk and regulatory requirements into a single decision-making framework. Its main advantage is that it treats the judicial information system as a sociotechnical and legally regulated environment in which security must protect not only data and infrastructure, but also the validity, traceability, and reliability of procedural actions.

The model is applicable when planning new systems, modernizing existing solutions, conducting internal checks, and preparing for audits in courts and prosecutor's offices, as well as in other administrative structures that process sensitive or classified information. By linking assets, risks, regulatory requirements, and control measures, it supports the consistency, justification, and traceability of decisions. This makes it a suitable basis for the development of institutional methodologies and for empirical verification in a real judicial environment.

The main contribution of the paper is the integration of risk assessment and regulatory compliance into a single decision-support model tailored to judicial information systems.

The model was not empirically validated through deployment in multiple courts, which is a limitation of the present study. Its verification was analytical and scenario-based. The purpose of this stage was to examine whether the proposed structure can consistently connect assets, risks, regulatory requirements, and security measures in typical judicial information system scenarios. Future research should focus on empirical validation through expert evaluation, pilot implementation, or comparative assessment across different judicial institutions.

REFERENCES

- [1] A. Maralbaeva, "Evolution of e-Justice Platforms: from ICT in Courts Towards 'Digital Justice' Portal in Kyrgyzstan," *International Journal for Court Administration*, vol. 15, no. 1, art. 6, 2024, <https://doi.org/10.36745/ijca.582>.
- [2] M. Fabri, "Will COVID-19 Accelerate Implementation of ICT in Courts?," *International Journal for Court Administration*, vol. 12, no. 2, art. 2, 2021, <https://doi.org/10.36745/ijca.384>.

- [3] J. Björkdahl and C. Kronblad, "Getting on track for digital work: Digital transformation in an administrative court before and during COVID-19," *Journal of Professions and Organization*, vol. 8, no. 3, pp. 374-393, 2021, <https://doi.org/10.1093/jpo/joab015>.
- [4] C. Kronblad and J. E. Pregmark, "When digitalization hit the court: Strategizing to turn turbulence into opportunities," *Journal of Professions and Organization*, vol. 12, no. 1, art. joae007, 2025, <https://doi.org/10.1093/jpo/joae007>.
- [5] O. Oktal, O. Alpu, and B. Yazici, "Measurement of internal user satisfaction and acceptance of the e-justice system in Turkey," *Aslib Journal of Information Management*, vol. 68, no. 6, pp. 716-735, 2016, <https://doi.org/10.1108/AJIM-04-2016-0048>.
- [6] M. Schmidt, "Information security risk management terminology and key concepts," *Risk Management*, vol. 25, art. 2, 2023, <https://doi.org/10.1057/s41283-022-00108-8>.
- [7] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, "Risk management practices in information security: Exploring the status quo in the DACH region," *Computers & Security*, vol. 92, art. 101776, 2020, <https://doi.org/10.1016/j.cose.2020.101776>.
- [8] National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST SP 800-39, 2011, <https://doi.org/10.6028/NIST.SP.800-39>.
- [9] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Rev. 1, 2012, <https://doi.org/10.6028/NIST.SP.800-30r1>.
- [10] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, 2022.
- [11] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*, 2022.
- [12] ISO 31000:2018, *Risk management - Guidelines*, 2018.
- [13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4 May 2016.
- [14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333, 27 December 2022.
- [15] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), OJ L 257, 28 August 2014.
- [16] Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, OJ L, 27 December 2023.
- [17] Cybersecurity Act, promulgated in State Gazette No. 94 of 13 November 2018, amended and supplemented in State Gazette No. 17 of 13 February 2026. [In Bulgarian].
- [18] Classified Information Protection Act, promulgated in State Gazette No. 45 of 30 April 2002. [In Bulgarian].
- [19] Ordinance on the Security of Communication and Information Systems, adopted by Council of Ministers Decree No. 28 of 24 February 2020, promulgated in State Gazette No. 18 of 28 February 2020. [In Bulgarian].
- [20] Ordinance No. 1 of 8 January 2008 on Automated Information Systems in the Judiciary. [In Bulgarian].
- [21] Rules on the Internal Procedure for the Use of Electronic Signatures and Electronic Identification by the Authorities of the Judiciary, adopted by the Plenum of the Supreme Judicial Council under item 39 of Protocol No. 10/16 March 2017, promulgated in State Gazette No. 32 of 21 April 2017. [In Bulgarian].
- [22] Ordinance No. 6 of 3 August 2017 on the Performance of Procedural Actions and Certifying Statements in Electronic Form, promulgated in State Gazette No. 67 of 18 August 2017, amended and supplemented in State Gazette No. 53 of 1 July 2025. [In Bulgarian].
- [23] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, 2024, <https://doi.org/10.6028/NIST.CSWP.29>.
- [24] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*, NIST SP 800-61 Rev. 3, 2025, <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [25] R. S. Alves, J. P. B. da Silva, L. A. Ribeiro Junior, and R. R. Nunes, "Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework," *Computers & Security*, vol. 157, art. 104584, 2025, <https://doi.org/10.1016/j.cose.2025.104584>.
- [26] I. V. Tîcovan and G. Sebestyen, "Solutions for enhancing the protection of digital evidence in judicial information systems," *Romanian Journal of Information Technology and Automatic Control*, vol. 35, no. 2, pp. 19-32, 2025, <https://doi.org/10.33436/v35i2y202502>.
- [27] M. Ramos-Maqueda and D. L. Chen, "The data revolution in justice," *World Development*, vol. 186, art. 106834, 2025, <https://doi.org/10.1016/j.worlddev.2024.106834>.

Artificial Intelligence Use in Professional Bachelor Thesis Writing: A Survey-Based Analytical Framework

Renata Kondratavičienė

Vilniaus kolegija / Higher

Education Institution

Vilnius, Lithuania

<https://orcid.org/0000-0001-5665-9726>

Abstract—This paper examines students' use of artificial intelligence (AI) in professional bachelor thesis writing and asks how those patterns can be described in a form useful for future support and governance in higher education. The study compared the 2024 and 2025 graduating classes at the same Lithuanian institution. The target population comprised 399 students, and the final sample included 258 respondents, with 129 from each graduating class. The questionnaire covered thesis-related tasks, named tools, perceived benefits and risks, attitudinal statements, and open-ended comments. Quantitative data were analysed in SPSS using frequencies, percentages, reliability analysis, Shapiro-Wilk tests, non-parametric comparisons, and Spearman correlations. Open-ended comments were grouped thematically. The results show a stable pattern: students used AI most often for paraphrasing and summarising, translation, grammar and style revision, and literature search. ChatGPT and Google Scholar clearly dominated the tool profile. Students valued AI mainly because it saved time and made writing easier to manage, but they also pointed to errors, weaker originality, and the need to verify AI-generated content. Lecturer guidance was the strongest attitudinal result, suggesting a practical need rather than a general wish for more regulation. The paper translates the survey evidence into a layered framework that separates student context, thesis tasks, named tools, perceived risks, and guidance expectations. This framework may inform later supervision dashboards, disclosure forms, or rule-based support systems for thesis administration. The study also identifies a limit in the available evidence: when reliable Lithuanian-language AI-detection data are not collected, self-reports and AI-use declarations should be treated as supervision and verification indicators, not as proof of misconduct.

Keywords—artificial intelligence, thesis writing, higher education, academic integrity, decision support, educational analytics

I. INTRODUCTION

Artificial intelligence entered thesis writing faster than universities managed to agree on clear rules for its use. In a professional bachelor thesis, this matters. A final thesis is tied to authorship, source use, method, and the public defence of one's own work. Students may use AI at different points in that process, but not all of those points carry the same academic weight. If institutions want workable guidance, they first need a clearer picture of where students actually use AI and what kind of help they expect from it.

Artificial intelligence entered thesis writing before universities had settled how to govern it. In the context of a professional bachelor thesis, this is not a technical add-on. The thesis is the document through which a student demonstrates the ability to select sources, make methodological choices, develop an argument, and defend the result. AI may support wording, searching, translation, and other limited steps, but those steps do not carry the same academic weight. This study therefore asks a deliberately concrete question: where, in theses that had already been defended, did students say AI had entered, and where did they still need guidance?

Recent research in higher education presents a mixed picture. On the one hand, students and teachers report practical benefits: AI can support wording, translation, summarising, feedback, and literature search [2]-[5]. On the other hand, the same literature identifies risks associated with integrity, disclosure, accuracy, and overreliance [6]-[11]. The discussion is therefore no longer simply about whether AI is present in academic work. The more difficult question is how it enters that work and where its boundaries should be drawn.

A less settled issue is the everyday pattern of AI use once a thesis has been written and defended. Much of the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.221>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

discussion remains general or policy-oriented, with less attention to the specific tasks for which students use AI, the tools they choose, and the points at which they still feel uncertain. Post-defence data are useful in this respect because they capture students' retrospective view of the whole writing process rather than one isolated moment within it.

The systems-design relevance of this paper is therefore practical. If a university later seeks to develop a rule-based guidance tool, a monitoring dashboard, or an AI-aware supervision system, it first needs clear input variables. Those variables do not begin with software; they begin with evidence about tasks, tools, risk signals, and guidance needs [14]-[16]. This study works at that requirements level.

II. THEORETICAL BACKGROUND

A. AI as Support in Academic Writing

Students rarely use AI for a single purpose. The same tool may help with rewording, translation, summarising, literature search, or a first idea for structuring text [2]-[5]. Academic writing, however, is not a single task. It combines language work, search, planning, method, and argument. For that reason, AI use has to be read in relation to the task itself, not only in relation to the tool.

A thesis makes this especially visible. Some tasks are close to technical support, such as improving wording or finding a better translation. Other tasks move much closer to academic ownership, such as shaping the topic, choosing a method, or interpreting data. Recent work in higher education increasingly stresses that AI may assist writing, but it cannot replace responsibility for the final academic text [3], [4], [6].

In this study, thesis writing is treated as a layered process. One layer concerns the task itself. Another concerns the tool used for that task. A third concerns how students judge benefits, risks, and acceptable use. This simple division makes the pattern easier to describe and later easier to translate into a usable support model.

B. Integrity, Disclosure, and Institutional Guidance

Current discussions about AI and academic integrity are no longer well captured by a simple allowed-or-forbidden distinction. Greater attention is now given to transparency, disclosure, and proportionate use [7], [10]-[11]. In practice, students need to understand not only whether AI is permitted, but also when its use becomes problematic for authorship, source work, or method.

Institutional guidance matters for the same reason. Clearer rules help students make better decisions, and they also make later governance tools more transparent. A technical system is easier to trust when the logic behind its categories reflects academic norms and when users can see why some practices are low risk while others require closer review [15], [16].

For that reason, this article considers use, evaluation, and guidance together. These are connected rather than separate issues. A student may use AI often while still

mistrusting its output; another may use it cautiously but still want clearer rules on originality or disclosure. The combination of task, tool, and attitude data is therefore especially important.

III. METHODOLOGY

A. Design

The study followed a comparative post-defence survey design. The same questionnaire was administered after the thesis defence period in two consecutive years, 2024 and 2025, in the same Lithuanian higher education institution. Students were asked how they had used AI during thesis preparation and how they evaluated that use after the process was finished. This made it possible to compare the 2024 graduating class with the 2025 graduating class while keeping the questions close to real thesis work.

B. Participants and Instrument

The target population comprised all students who defended a professional bachelor thesis in the two years under review: 198 in 2024 and 201 in 2025. A finite-population sample-size benchmark at 95% confidence and a 5% margin of error suggested a minimum of 196 responses. The study obtained 258 valid responses, 129 from the 2024 graduating class and 129 from the 2025 graduating class. The questionnaire followed the logic of thesis preparation. It began with background questions on study mode, funding, and study programme (A1-A3). It then moved to the task-related AI-use block (A4), which asked how often AI was used in eleven thesis-writing tasks, and the tool-use block (A5), which listed named systems and platforms. Two open-response blocks invited students to describe actual practice (A6) and expected guidance (A10). Between them, the benefits block (A7), the drawbacks block (A8), and the attitudinal block (A9) captured how students judged usefulness, risk, and institutional support.

TABLE I. SAMPLE ADEQUACY BENCHMARK AND ACHIEVED SAMPLE

Graduating class	Population	Achieved n
2024	198	129
2025	201	129
Total	399	258

Benchmark n was estimated using the finite-population sample-size formula at 95% confidence and a 5% margin of error.

As shown in Table I, the achieved sample was sufficient in aggregate and balanced across the two graduating classes. This gives the comparison a stable descriptive basis. At the same time, the study remains a single-institution survey based on voluntary participation, so the results should be read as informative rather than directly generalisable.

The questionnaire structure also supports content validity. It moved from background characteristics to task-level AI use, then to tools, evaluation, and guidance. Students were therefore not asked about AI in the abstract, but in a sequence that reflects how thesis work is usually experienced.

C. Data Analysis

Quantitative data were analysed in SPSS. Frequencies and percentages were calculated for background variables, the task-related AI-use block (A4), the tool-use block (A5), and selected indicators from the benefits and drawbacks blocks (A7 and A8). For the task-related AI-use block (A4) and the attitudinal block (A9), internal consistency was checked with Cronbach's alpha [13]. Shapiro-Wilk tests were used to assess distributional shape. Because the index distributions departed from normality, non-parametric procedures were preferred, and associations were examined using Spearman's rho.

Open-ended responses were grouped thematically through repeated reading, coding, and theme refinement in line with Braun and Clarke's approach [12]. This made it possible to retain the practical detail of student comments while still presenting the material in an organised way.

The task-related AI-use block (A4) and the tool-use block (A5) used the same five-point frequency scale from 1 (never) to 5 (always). The benefits block (A7) and the drawbacks block (A8) were coded as binary multiple-response indicators because respondents could select more than one option. The attitudinal block (A9) used a five-point agreement scale, and the open-response blocks (A6 and A10) were retained for thematic analysis. This coding strategy made it possible to move from broad patterns to more focused analytical links between tasks, tools, and governance signals.

D. Institutional Verification Context and Data Triangulation

To place the survey data in relation to institutional procedure, the final-thesis submission route was reviewed together with the questionnaire results. In the analysed institution, final theses were submitted through the Moodle virtual learning environment, and Turnitin was integrated into that workflow. The system therefore provided a formal route for similarity and originality checking during thesis submission.

Turnitin did not, however, provide a reliable basis for detecting AI-generated Lithuanian-language text in final theses during the period under review. For that reason, the institution did not produce a comparable register showing how many students were not admitted to defence, how many theses were rejected, or how many sanctions were imposed specifically because of unauthorised AI use. The paper therefore avoids reporting figures that the institutional evidence could not support.

The available institutional reference point was therefore procedural rather than numerical. Under the institution's guidelines for AI use in written assignments, and in line with broader ethical guidance on AI in study processes [11], students include an AI-use declaration in the final thesis. The survey findings are consequently interpreted as anonymous post-defence self-reports, read alongside a disclosure requirement, rather than as a disciplinary audit.

E. Engineering Relevance of the Analytical Model

The study does not present a deployed software tool. Its engineering contribution is preliminary: it organises the survey data into variables that a later tool could use in practice. The analytical model links four layers: student context (A1-A3), task-related use (A4), named tools (A5), and governance evidence drawn from benefits, risks, attitudes, and open comments (A7-A10). This ordering follows the thesis process itself, from student context to the tasks performed, the tools named, and the points at which clearer safeguards were expected.

For systems design, this boundary is useful rather than problematic. A dashboard, disclosure checklist, or rule-based guidance tool would gain little from a single overall attitude score. It would require separable signals: routine language support, limited use in topic and data work, reliance on a few familiar platforms, and explicit requests for rule clarification. The article stops before implementation, but identifies the type of evidence that implementation would require [14]-[16].

F. Validity, Reliability, Ethics, and AI-Use Disclosure

The questionnaire was researcher-developed, so its main strength lies in its close fit with the study aim and with the real sequence of thesis preparation. Content validity was supported by the instrument's progression from background variables to tasks, tools, benefits, risks, attitudes, and open comments. Internal consistency was checked for the task-use block (A4) and the attitudinal block (A9). The pooled alpha was .892 for A4 and .869 for A9, while year-specific alphas were also strong. This supports the use of composite indicators for careful interpretation.

The tool-use block (A5) produced an alpha of .797 in the pooled dataset, but this was not treated as evidence of a single latent scale. The block lists different kinds of tools, from chat-based systems to search tools and citation software. For that reason, A5 was interpreted mainly as a tool-use profile rather than as a single construct.

The survey was anonymous and voluntary, and the findings are reported only in aggregated form. Open-ended answers were used as contextual evidence and were not treated as material that could identify individual respondents. Participation implied consent to the use of responses for research and educational improvement purposes.

Because the paper itself deals with acceptable AI use in academic work, AI-use disclosure was treated as part of the methodology. OpenAI ChatGPT was used only for language editing and wording revision during manuscript preparation. It was not used to generate the survey data, run SPSS procedures, or produce the empirical results. The author reviewed all interpretations and retains full responsibility for the final text.

IV. RESULTS

A. Respondent Profile

To describe the two graduating classes and the study contexts represented in the dataset, the background variables were examined (see Table II).

TABLE II. RESPONDENT PROFILE

Characteristic	2024	2025
Part-time	41	15
Full-time	38	54
Full-time sessional	50	60
State-funded	88	84
Self-funded	41	45
Primary Education	29	33
Childhood Pedagogy	63	63
Social Work	37	33

Values are frequencies.

Table II shows that the two graduating classes were equal in size but not identical in composition. The 2024 graduating class included more part-time students (31.8%) than the 2025 graduating class (11.6%), whereas the 2025 graduating class had more full-time students. Programme composition was more stable: Childhood Pedagogy was the largest group in both years, while Primary Education and Social Work were represented in smaller but still comparable numbers. Funding structure was also similar across the two year groups.

This matters for the year comparison. The two graduating classes were not identical populations. The main structural shift concerned study mode. Later differences in AI use should therefore be read as differences between year groups within a broadly similar study environment, not as evidence of two wholly different student populations.

B. Thesis-Related Tasks in Which AI Was Used Most Often

To see in which parts of thesis writing AI was used most often, the task-related AI use block (A4) was examined (see Table III).

TABLE III. TASK-LAYER INDICATORS OF AI USE IN THESIS WRITING

Task	2024	2025	All
Topic selection	1.40	1.47	1.44
Literature search	1.96	2.00	1.98
Structure/content	1.71	1.81	1.76
Text generation	1.58	1.72	1.65
Grammar/style	1.87	2.33	2.10
Research gaps/errors	1.74	1.56	1.65
Text analysis	1.64	1.72	1.68
Paraphrase/summarise	2.27	2.35	2.31
Data collection/analysis	1.71	1.44	1.58
Translation	2.12	2.56	2.34
Plagiarism check	1.84	1.30	1.57

Mean values are based on the five-point frequency scale from 1 = never to 5 = always.

Table III shows a clear and stable pattern. In both year groups, AI use was strongest in language-related and search-related tasks rather than in the more conceptually sensitive parts of thesis writing. The highest means were found for paraphrasing and summarising (2.27 in 2024 and

2.35 in 2025), translation (2.12 and 2.56), grammar and style revision (1.87 and 2.33), and literature search (1.96 and 2.00). These results suggest that students mainly used AI to improve wording, polish text, and support source work.

The lower end of Table III is as informative as the top. Topic selection stayed low in both cohorts, and data collection or analysis also remained near the lower end of the scale. Plagiarism-related use was moderate in 2024 and lower in 2025. These are not merely low scores; they mark the parts of thesis preparation in which authorship, evidence, and formal accountability are most directly implicated.

The year-to-year difference is therefore better described as a shift in emphasis. In 2025, language correction and translation gained weight; in 2024, data-related help and plagiarism checking appeared somewhat more often. The overall shape of use, however, remained stable.

C. Students' Own Descriptions of AI Use

Students' open-ended responses to the question "Please describe in more detail how you typically used AI software during the process of writing your professional bachelor's thesis" help explain how the quantitative results were reflected in everyday thesis-writing practices. Students described AI as a tool for rephrasing sentences, shortening or clarifying passages, translating text, checking language, sketching a structure, and locating sources. Several comments suggested a narrower use still: the idea already belonged to the student, but AI helped find the first formulation.

The comments do not support a picture of simple copying from a chatbot into the thesis. Respondents referred instead to checking, rewriting, selecting, and treating generated wording as draft material. This detail matters because it places AI in an editorial support role while leaving responsibility for the final wording with the student.

D. Most Frequently Used Tools

To identify which tools shaped students' AI use most clearly, the tool-use block (A5) was examined (see Table IV).

TABLE IV. TOOL-LAYER PROFILE OF AI USE

Tool	2024	2025	All
ChatGPT	2.75	2.91	2.83
Google Scholar	2.36	2.67	2.52
Gemini	1.49	1.16	1.33
Grammarly	1.33	1.21	1.27
Turnitin	1.35	1.19	1.27
SPSS	1.33	1.00	1.17
Mendeley	1.19	1.00	1.10
Zotero	1.09	1.05	1.07

Mean values are based on the five-point frequency scale from 1 = never to 5 = always.

Table IV shows a highly concentrated tool profile. In both year groups, ChatGPT and Google Scholar stood clearly above the rest. ChatGPT had the highest mean in both years (2.75 in 2024 and 2.91 in 2025), while Google Scholar followed (2.36 and 2.67). The remaining tools stayed much closer to the lower end of the scale.

This suggests that students did not build a broad or diversified tool environment around thesis writing. Instead, reported activity clustered around a small number of familiar tools. The 2025 profile appears, if anything, even more concentrated than the 2024 profile.

The distribution adds an important detail. In 2024, some respondents had never used ChatGPT, although a group of regular users was already visible. In 2025, non-use became less common and repeated use became more routine. Google Scholar moved in the same direction, but more gradually. SPSS, Mendeley, Zotero, Grammarly, and Turnitin remained marginal in students' accounts of AI-assisted writing. Turnitin requires careful interpretation here: it belonged to the Moodle-based institutional checking route, but students did not describe it as a tool they used to compose or revise their theses.

E. Perceived benefits, risks, and evaluative attitudes

To understand how students weighed benefits against risks and what kind of guidance they expected, selected indicators from the benefits block (A7), the drawbacks block (A8), and the attitudinal block (A9) were reviewed together (see Table V).

TABLE V. BENEFIT, RISK, AND ATTITUDE INDICATORS RELEVANT TO AI GOVERNANCE

Indicator	2024	2025	All
Time saving	0.70	0.51	0.61
Productivity	0.39	0.33	0.36
Quality gain	0.33	0.42	0.38
Possible errors	0.76	0.70	0.73
Reduced originality	0.50	0.42	0.46
Needs extra knowledge	0.46	0.40	0.43
Recommend AI	3.33	3.42	3.38
Use in theses	3.31	3.35	3.33
Lecturer guidance	3.88	4.19	4.03

Benefit and risk indicators are proportions; attitudinal indicators are mean scores on a five-point agreement scale.

Table V presents a balanced picture. Among the benefits, time saving was the strongest response in both year groups, especially in 2024. Productivity and perceived quality gains were also visible, although less prominent. Among the risks, possible errors were the dominant concern in both years, followed by reduced originality and the need for additional knowledge when working with AI.

The attitudinal items point in the same direction. Students were neither clearly resistant to AI nor uncritically enthusiastic. Agreement was moderate for recommending AI and for its use in thesis writing, but it was strongest for lecturer guidance. This item reached 3.88 in 2024 and 4.19 in 2025, making it the clearest single signal in the attitudinal block.

Taken together, the results indicate careful use rather than enthusiasm for AI as such. Students valued speed and help with drafting, but their responses repeatedly returned to errors, originality, and verification. Their request for guidance therefore reads as a request for usable boundaries: how to work with familiar tools without weakening authorship or academic accountability.

F. Reliability, Distribution, and the Link Between Use and Attitude

To check whether the composite indicators derived from the task-use block (A4) and the attitudinal block (A9) were stable enough for interpretation and to see whether use and attitude moved together, reliability, distribution, and association results were reviewed (see Table VI).

TABLE VI. RELIABILITY, NORMALITY, AND ANALYTICAL ASSOCIATIONS

Indicator	2024	2025	All
Task-use block (A4) alpha	.917	.858	.892
Attitudinal block (A9) alpha	.880	.854	.869
AI use mean	1.80	1.84	1.82
Attitude mean	3.51	3.65	3.58
SW p: AI use	< .001	< .001	-
SW p: attitude	< .001	< .001	-
Spearman rho	.536***	.447***	-

*** p < .001. Shapiro-Wilk results are reported separately for each graduating class.

Table VI shows that both composite indicators were sufficiently stable for cautious interpretation. The task-use block (A4) reached alpha values of .917 in 2024, .858 in 2025, and .892 in the pooled sample. The attitudinal block (A9) also showed good internal consistency (.880, .854, and .869 respectively). The mean AI-use index remained low to moderate in both year groups (1.80 and 1.84), while the attitude index was higher and more stable (3.51 and 3.65).

The distribution tests are also relevant. Shapiro-Wilk results were significant for both indices in both year groups, indicating a departure from normality. This supports the choice of non-parametric procedures. In practice, the year comparison was therefore read cautiously. The descriptive tables showed some shifts in emphasis, but not a break in the overall logic of AI use.

The association results were more informative. In 2024, the link between the AI-use index and the attitude index reached rho = .536; in 2025, it reached rho = .447. The broader correlation matrices pointed in the same direction: tool use tended to align with the tasks for which those tools are best suited. Analytically, this matters because it shows that the model is not only descriptive. The variables also move together in a way that could support later rule-based or AI-assisted supervision logic [14]-[16].

G. What Guidance Did Students Expect from Thesis Organisation?

To understand what students expected from supervisors and thesis organisers, the open comments on guidance from the final open-response block (A10) were grouped into themes (see Table VII).

TABLE VII. OPEN-COMMENT THEMES RELEVANT TO GUIDANCE DESIGN

No.	Theme
1	Clear rules and boundaries
2	Practical training and examples
3	Verification of AI-generated material
4	AI as support, not substitution
5	Disclosure and originality

Themes were derived from open-ended responses and summarised in English by the author.

Table VII shows that students wanted practical clarity rather than abstract policy. The most common requests concerned clearer rules and boundaries, examples of acceptable use, stronger emphasis on checking AI-generated material, and a clear message that AI should support rather than replace student work.

Table VII shows that students wanted practical clarity rather than abstract policy. The most common requests concerned clearer rules and boundaries, examples of acceptable use, stronger emphasis on checking AI-generated material, and a clear message that AI should support rather than replace student work.

The comments from the two year groups were similar in tone, but the later group expressed the need for procedural clarity more strongly. Students wanted lecturers to explain what could be done, what had to be reported, and how much rewriting or checking was expected when AI had been used.

Read together with Table V, these comments explain why lecturer guidance became the strongest attitudinal item in the whole study. Students were not only using AI; they were also asking institutions to state more clearly how that use should be handled in everyday thesis work.

V. DISCUSSION

The findings show that AI had already become part of thesis-writing practice, although in a limited and recognisable way. Students used it most often for paraphrasing, translation, grammar and style revision, and literature search. Much less use was reported in tasks closer to topic ownership, data work, or formal control. This suggests a fairly clear boundary in students' own practice between support functions and academically sensitive functions.

The tool profile reinforces that interpretation. ChatGPT and Google Scholar clearly dominated, while specialised tools remained secondary. This is consistent with studies showing that actual student use often concentrates around a small number of accessible platforms rather than around a large and evenly used ecosystem [3]-[5]. From a practical viewpoint, students seem to prefer tools that fit easily into writing and searching routines they already know.

The evaluative results also fit recent integrity and policy discussions. Students valued AI because it saved time and made writing easier to manage, but they also identified errors, weaker originality, and the need for verification [6]-[11]. This is not blind enthusiasm. It is closer to cautious adoption: students are willing to use AI, but they do not fully trust it and still expect institutions to define clearer boundaries.

From a systems perspective, the study does not argue for automated judgement about student writing. Its contribution is more modest and, in this context, more realistic. The results identify a usable set of variables for future support tools: task-sensitive indicators, tool profiles, and governance cues drawn from perceived risks and

guidance needs. A future system built on this logic would not replace supervisors. Its role would be to support them with clearer signals and more consistent guidance.

Several limitations should be kept in mind. The study was conducted in one institution and relied on voluntary self-report after thesis defence. It therefore reflects students' remembered practice rather than direct observation of writing behaviour. The paper also does not test a deployed AI system, so its engineering contribution remains at the analytical and requirements level. This limitation is important rather than incidental: weak variables lead to weak tools.

The main triangulation limit is institutional, not merely methodological. In the period analysed, final theses passed through Moodle and a Turnitin-supported checking workflow. That workflow did not yield reliable Lithuanian-language AI-detection data for final theses. As a result, no comparable institutional register existed for AI-related thesis rejections, non-admissions to defence, or sanctions in the two cohorts. The study therefore cannot test self-reports against such records. It can show, however, why AI-use declarations, supervisor reading, and task-sensitive verification become important when automated evidence is unavailable.

At the institutional level, a policy statement is only a starting point. Thesis supervision also needs working rules: which uses of AI are acceptable, when they must be declared, and which parts of the thesis require closer human review because students' ownership of argument, sources, or data may be affected.

A first support tool could be simple. It could ask students to indicate whether AI was used for translation, language editing, source searching, or idea development; link each answer to a short guidance note; and show supervisors where closer review is advisable. The present data suggest that such prompts should focus on language polishing, translation, literature search, and uncertain cases in which students do not know whether rewriting, checking, or acknowledgement is required.

VI. CONCLUSION

This study showed that AI was already part of professional bachelor thesis writing at the surveyed Lithuanian institution, but mainly as a support tool for wording, translation, grammar and style revision, and literature search. Students did not report equally strong use across all thesis tasks, which suggests that they still distinguished between low-risk support and tasks that remained more clearly their own responsibility.

The comparison between cohorts should therefore be read cautiously. The 2025 cohort gave slightly more weight to translation and language correction, but the same task structure remained visible in both years. Tool use also remained narrow: ChatGPT and Google Scholar stood apart from the rest.

The practical conclusion is pedagogical as much as technical. Students expected lecturers to explain which AI uses are acceptable in thesis preparation, how such use

should be disclosed, and which uses still require verification. For the conference audience, the paper offers not a finished technical artefact but a compact analytical framework for later AI-aware supervision or decision-support systems. Its main caution is also clear: when reliable language-specific AI-detection statistics are unavailable, governance should combine declared use, supervisor review, and task-sensitive verification rather than rely on automated detection alone.

REFERENCES

- [1] UNESCO, Guidance for Generative AI in Education and Research. Paris, France: UNESCO, 2023.
- [2] H. Crompton and D. Burke, "Artificial intelligence in higher education: The state of the field," *International Journal of Educational Technology in Higher Education*, vol. 20, art. no. 22, 2023, <https://doi.org/10.1186/s41239-023-00392-8>
- [3] M. I. Baig and E. Yadegaridehkordi, "ChatGPT in higher education: A systematic literature review and research challenges," *International Journal of Educational Research*, vol. 127, art. no. 102411, 2024, <https://doi.org/10.1016/j.ijer.2024.102411>
- [4] A. Barrett and A. Pack, "Not quite eye to A.I.: Student and teacher perspectives on the use of generative artificial intelligence in the writing process," *International Journal of Educational Technology in Higher Education*, vol. 20, art. no. 59, 2023, <https://doi.org/10.1186/s41239-023-00427-0>
- [5] C. K. Y. Chan and W. Hu, "Students' voices on generative AI: Perceptions, benefits, and challenges in higher education," *International Journal of Educational Technology in Higher Education*, vol. 20, art. no. 43, 2023, <https://doi.org/10.1186/s41239-023-00411-8>
- [6] D. R. E. Cotton, P. A. Cotton, and J. R. Shipway, "Chatting and cheating: Ensuring academic integrity in the era of ChatGPT," *Innovations in Education and Teaching International*, vol. 61, no. 2, pp. 228-239, 2024, DOI: 10.1080/14703297.2023.2190148.
- [7] C. K. Y. Chan, "A comprehensive AI policy education framework for university teaching and learning," *International Journal of Educational Technology in Higher Education*, vol. 20, art. no. 38, 2023, <https://doi.org/10.1186/s41239-023-00408-3>
- [8] J. Delcker, J. Heil, D. Ifenthaler, S. Seufert, and L. Spirgi, "First-year students' AI competence as a predictor for intended and de facto use of AI tools for supporting learning processes in higher education," *International Journal of Educational Technology in Higher Education*, vol. 21, art. no. 18, 2024, <https://doi.org/10.1186/s41239-024-00452-7>
- [9] D.-K. Mah and N. Gross, "Artificial intelligence in higher education: Exploring faculty use, self-efficacy, distinct profiles, and professional development needs," *International Journal of Educational Technology in Higher Education*, vol. 21, art. no. 58, 2024, <https://doi.org/10.1186/s41239-024-00490-1>
- [10] H. Wang, A. Dang, Z. Wu, and S. Mac, "Generative AI in higher education: Seeing ChatGPT through universities' policies, resources, and guidelines," *Computers and Education: Artificial Intelligence*, vol. 7, art. no. 100326, 2024, <https://doi.org/10.1016/j.caeai.2024.100326>
- [11] Office of the Ombudsperson for Academic Ethics and Procedures of the Republic of Lithuania, "On approving guidelines for the ethical use of artificial intelligence in research and study processes (Order No. V-14)," Apr. 29, 2024. [Online]. Available: <https://e-tar.lt/portal/lt/legalAct/56254af0061111efbcbfb318996800a8>
- [12] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006, <https://doi.org/10.1191/1478088706qp063oa>
- [13] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297-334, 1951, <https://doi.org/10.1007/BF02310555>
- [14] G. Siemens and R. S. J. d. Baker, "Learning analytics and educational data mining: Towards communication and collaboration," in *Proc. 2nd Int. Conf. Learning Analytics and Knowledge (LAK '12)*, Vancouver, BC, Canada, 2012, pp. 252-254, <https://doi.org/10.1145/2330601.2330661>
- [15] H. Khosravi, S. Buckingham Shum, G. Chen, C. Conati, Y.-S. Tsai, J. Kay, S. Knight, R. Martinez-Maldonado, S. Sadiq, and D. Gasevic, "Explainable artificial intelligence in education," *Computers and Education: Artificial Intelligence*, vol. 3, Art. no. 100074, 2022, <https://doi.org/10.1016/j.caeai.2022.100074>
- [16] M. Bond, H. Khosravi, M. de Laat, N. Bergdahl, V. Negrea, E. Oxley, P. Pham, S. W. Chong, and G. Siemens, "A meta systematic review of artificial intelligence in higher education: A call for increased ethics, collaboration, and rigour," *International Journal of Educational Technology in Higher Education*, vol. 21, Art. no. 4, 2024, <https://doi.org/10.1186/s41239-023-00436-z>

Methods and Models for Image Enhancement in Low-light Conditions

Mariia Liashenko

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
mariia.liashenko@nure.ua

Kirill Smelyakov

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
kirylo.smelyakov@nure.ua

Anastasiya Chupryna

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
anastasiya.chupryna@nure.ua

Dainius Savulionis

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
d.savulionis@eif.viko.lt

Loreta Savulioniene

Faculty of Economics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
l.savulioniene@viko.lt

Paulius Sakalys

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
p.sakalys@eif.viko.lt

Abstract— This article reviews current research on various approaches to improving images captured in low-light or dimly lit conditions. To address this issue, an adaptive ensemble method is proposed that combines several, specifically, four classical image processing algorithms and automatically distributes weights among them based on local quality. The developed system uses CLAHE, gamma correction, the Retinex algorithm, and automatic contrast stretching as its basic components. A comparative analysis of the developed method with the modern Deep Learning approach, Zero-DCE, was conducted on the real-world LOL dataset. The experimental results show that the proposed classical ensemble approach achieves a PSNR of 17.91 dB, outperforming the machine learning model by 14.2 percent, while the method does not require a training phase on datasets or GPU computations.

Keywords—image enhancement, low-light enhancement, ensemble methods, CLAHE, Zero-DCE, adaptive weighting, image processing.

I. INTRODUCTION

In daily life, some fields require high-quality and clear images, such as biomedicine, aerospace, transportation, military, etc. But sometimes, the shooting will be affected by the environment or the equipment used, resulting in the inability to capture clear and high-quality images.[1][2]

Image recognition is usually presented as a multi-class classification problem in which the identification of a relevant set of specific features which performs best is a difficult task [3].

This challenge has a wide range of practical applications across many fields, from mobile photography and video surveillance systems to autonomous vehicle control systems and medical imaging. The main problems that can arise when working with such images include a very low signal-to-noise ratio, high noise levels from camera sensors, significant loss of detail in shadowed areas, and a significant distortion of the natural color reproduction of objects in the image.

Current research in this field can be broadly divided into two main methodological categories. The first category includes classical image processing methods based on mathematical models and heuristic approaches. These methods are characterized by the clarity of their results, do not require significant computational resources, and can be effectively applied without a pre-training phase. However, the drawbacks of such methods include frequently limited result quality when processing complex scenes with uneven lighting, high noise levels, or a wide dynamic range.

The second category consists of deep learning-based approaches that have recently achieved impressive results across a variety of image processing tasks. Convolutional neural network models can capture complex nonlinear relationships between images captured under low-light and normal lighting conditions, enabling high-quality image enhancement. At the same time, such approaches require large amounts of paired training data and significant computational resources for training, and are

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.216>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

characterized by limited interpretability of their internal processes.

The aim of this study is to develop and investigate an ensemble approach to improving images captured in low-light conditions that combines the advantages of classical algorithms via adaptive weighting. The study also aims to conduct a thorough comparative analysis of the proposed method against modern machine learning approaches using real-world datasets.

II. REVIEW OF EXISTING SOLUTIONS

A. Heading Classical image processing methods

The CLAHE (Contrast Limited Adaptive Histogram Equalization) algorithm is an image processing technique designed to enhance local contrast, particularly in images with very dark or bright regions.[4] CLAHE divides the input image into rectangular blocks of fixed size and applies an equalization procedure to each block. The transformation can be written as (1):

$$J_k = (CDF(T_k) - CDF(min)) * \frac{(L-1)}{CDF(max) - CDF(min)} \quad (1)$$

where J_k is the equalized intensity value, T_k is the original pixel intensity, $CDF(\cdot)$ denotes the cumulative distribution function, and L is the number of possible intensity levels.

A critical feature of the method is the limitation of the maximum contrast enhancement factor via the clip limit parameter, which helps avoid excessive noise amplification in relatively homogeneous image regions. The method demonstrates high effectiveness in enhancing local details and textures, but may introduce increased noise in dark image areas if the parameters are set incorrectly.

Retinex, is a commonly used image enhancement method based on scientific experiments and analysis. The theory of Retinex is based on the idea that the color of an object is determined by its ability to reflect long-wave (red), medium-wave (green), and short-wave (blue) illumination rather than the absolute value of the reflected light. [5] The Single-Scale Retinex algorithm estimates the illumination component by applying a Gaussian filter with a large smoothing radius to the logarithm of the input image. By subtracting the logarithm of the estimated illuminance from the logarithmic representation of the input image, we obtain the reflection component, which effectively corresponds to the enhanced image. The parameter σ of the Gaussian filter determines the scale of the illuminance estimation and significantly affects the final quality of the result. The model is expressed as (2):

$$\begin{aligned} \log R(x, y) &= \log I(x, y) - \log L(x, y) \\ L(x, y) &= F * \log I(x, y) \\ F &= \text{Gaussian}(\sigma) \end{aligned} \quad (2)$$

where $R(x, y)$ is the reflectance component, $I(x, y)$ is the input image, $L(x, y)$ is the estimated illumination, F is a

Gaussian smoothing filter, and σ controls the scale of illumination estimation.

Gamma correction is a crucial process in digital imaging systems, aiming to compensate for the nonlinear relationship between input signal and luminance output. [6] The gamma correction method applies a nonlinear power transformation to pixel intensities. This means raising the normalized intensity to the inverse of the gamma parameter. When gamma values exceed 1, brightness increases primarily in dark areas of the image, while bright areas undergo minimal change, helping preserve contrast. The simplicity of the method and its low computational complexity make it attractive for real-time applications; however, a single global gamma parameter does not allow adaptation to local features of the illumination distribution in different parts of the image. The transformation is defined as (3):

$$I_{out} = 255 \cdot \left(\frac{I_{in}}{255} \right)^{\frac{1}{\gamma}} \quad (3)$$

where I_{in} is the input pixel intensity, I_{out} is the corrected intensity, and γ is the gamma parameter controlling the strength of the brightness adjustment.

The automatic contrast stretching method, linearly expands the original digital values of the remotely sensed data into a new distribution. By expanding the original input values of the image, the total range of sensitivity of the display device can be utilized. [7] In the first stage, the image's dynamic range is evaluated, typically using histogram percentiles to exclude outliers. After that, the interval between the defined boundaries is linearly stretched to cover the full range of possible intensity values. Using percentiles instead of absolute minimum and maximum values makes the method more robust against isolated excessively dark or bright pixels, which may be caused by noise or artifacts. The method effectively utilizes the entire available dynamic range of the display or storage system, but does not account for local features of the contrast distribution.

B. Deep Learning-Based Approaches

The Zero-DCE model trains the parameters of curves used for stepwise brightness correction at the pixel level. Architecturally, it consists of seven convolutional layers, each generating eight sets of curve parameters for iterative application to the input image. Within each iteration, a quadratic transformation is performed, which is determined by the corresponding curve parameters. It can cope with diverse lighting conditions including nonuniform and poor lighting cases. [8] The model contains approximately 79,000 parameters and exhibits very fast inference. A critical feature of Zero-DCE is its unsupervised training mode, which does not require paired low-light and normal-light image data. Instead, the model is trained using a combination of four specialized loss functions. Color instability is used to maintain the natural balance of color components in the enhanced image. Loss of exposure control ensures brightness level correction by

bringing the average intensity of local areas closer to a specified optimal level. Loss of lighting smoothness helps create a uniform brightness distribution within the scene and prevents sudden lighting changes. The Spatial Consistency Loss maintains the spatial structure similarity between the input and output images. This approach allows the model to be trained even in the absence of paired data, which is a significant advantage in practical applications.

C. Ensemble Approaches in Image Processing

Ensemble methods combine the results of several algorithms to obtain a more stable and accurate final result than any single method can provide. Compared to standalone single-network systems the proposed ensemble methodology blends sequential and parallel processing methods to produce an optimized enhancement performance. [9] In image processing tasks, this is most often achieved through weighted aggregation of the outputs of base models or algorithms. In this context, weighting coefficients can be determined empirically, optimized using validation data, or calculated based on the quality metrics of each individual method. This approach makes it possible to offset the shortcomings of some algorithms with the strengths of others, which ultimately improves the overall robustness and quality of the final result, especially when working with heterogeneous input data. More sophisticated adaptive methods evaluate the quality of each model's results locally for different parts of the image and dynamically determine optimal weights for each spatial location. This adaptability allows for the automatic selection of the best method for the specific characteristics of a local region of the image. However, early implementations of adaptive ensembles often suffered from visible pixelation artifacts, arising from abrupt weight transitions between neighboring image blocks during block-wise quality estimation without sufficient smoothing.

III. PROPOSED METHOD

A. Ensemble System Architecture

The SmoothAdaptive Ensemble system combines four classical image processing algorithms into a single ensemble structure, supplemented by a mechanism for adaptively weighting the results. The first component is based on the CLAHE method with an adjustable contrast threshold and local block size, allowing for enhancing local contrast without excessively increasing noise artifacts. The second component applies gamma correction with a typical coefficient to enhance the brightness of images captured in challenging low-light conditions. The third component implements the Single Scale Retinex algorithm using a large-scale Gaussian filter, which allows for the estimation of the spatial distribution of scene illuminance and ensures more accurate extraction of the reflection component.[11] The fourth component performs automatic contrast stretching by clipping 2% of the pixels at both ends of the histogram to improve robustness against outliers. This combination of methods covers a range of image

enhancement techniques, from local contrast to global tonal mapping.

B. Detailed Algorithm for Adaptive Weighting

The adaptive weighting process consists of five sequential stages, each of which is crucial for obtaining the final result. In the first stage, the input image is processed simultaneously by all four base models, which operate independently. Each model performs its own image transformation, resulting in four intermediate results that reflect different approaches to image enhancement.

In the second step, a spatial map of local quality is computed for each of the four intermediate results. This process is implemented by dividing the image into overlapping blocks measuring 128 by 128 pixels with a step size of 64 pixels, ensuring 50% overlap between adjacent blocks. Two quality metrics are calculated for each block. The first metric is based on the standard deviation of pixel intensities within the block, reflecting local contrast and the presence of detail. The second metric is the average gradient within the block, computed using the Sobel operator and reflecting the sharpness of edges and textures. The combined quality score for a block is computed as a weighted sum of the normalized standard deviation and the average gradient, with weights of 1/50 and 1/100, respectively. A critical step is to apply Gaussian smoothing to the resulting quality map with a kernel size of 99×99 pixels and a sigma parameter of 30. This smoothing eliminates abrupt transitions between the quality estimates of neighboring blocks, a key factor in preventing pixelation artifacts.

In the third step, the quality maps are normalized to calculate spatially variable weights. For each spatial location in the image, the four quality values from the different models are normalized so that their sum equals one. This transformation allows the weights to be interpreted as probabilities or relative contributions of each model to the final result for a given spatial location. After the initial normalization, an additional Gaussian smoothing with a kernel of 51 by 51 pixels and a sigma parameter of 15 is applied to each of the four weight maps. This second smoothing further smooths the spatial transitions of the weights. After smoothing, the weights are renormalized to restore the condition that their sum at each point equals one. This double-smoothing procedure is an innovative aspect of the developed method and is critical for achieving visually smooth results without blocky artifacts.

In the fourth step, an adaptive weighted merge of the four intermediate results is performed using the calculated spatially variable weights. For each spatial location in the image and for each color channel, the final intensity value is calculated as the weighted sum of the corresponding values from the four intermediate results. The weights used in this combination are spatially variable and automatically adjusted based on the local quality of the results from the different models. This means that across

different parts of the image, the final result may be closer to that of different base models, depending on which performs best in that area.

In the fifth and final step, post-processing of the final result is performed. Intensity values that may exceed the acceptable range due to smoothing and combination operations are clipped to a range from zero to two hundred fifty-five. The result is converted to an unsigned 8-bit integer, which is the standard image format. The final image is saved in JPEG format with a high quality level of 95% to minimize compression loss.

IV. EXPERIMENTAL STUDY

A. Experimental Methodology and Evaluation Metrics

To objectively verify the effectiveness of the proposed method, the LOL dataset was selected, which is one of the standard test sets in the tasks of improving images obtained under low-light conditions. It contains five hundred pairs of images, where each pair represents one scene recorded both in a dark environment and in normal light. The majority of the set, namely four hundred and eighty-five pairs, is used for training the models, while the remaining fifteen pairs are used for final quality testing. All images are real photographs taken in natural conditions without synthetic generation, which increases the realism of the experiments and allows for a correct assessment of the method's performance in practical scenarios.

For quantitative analysis of the quality of enhancement, a set of four widely accepted metrics was used, each characterizing a specific aspect of visual quality. The peak signal-to-noise ratio evaluates the accuracy of the reconstruction by comparing the enhanced image to a reference image of normal illumination, and higher values of this metric correspond to better reconstruction quality. The structural similarity index measures the degree of perceptual similarity between images, taking into account local brightness, contrast, and structural characteristics, where values close to unity indicate high similarity. The entropy determines the amount of information content of an image based on the distribution of pixel intensities, with higher values indicating a more detailed and informative image. The average gradient metric evaluates image sharpness by measuring the intensity of spatial changes across the image, highlighting edges and textures by computing horizontal and vertical gradients with the Sobel operator and averaging their magnitudes over the entire image.

B. Results of comparison of improvement methods

Figure 1 illustrates representative enhancement examples from the LOL dataset.



Figure 1. Visual comparison of low-light enhancement results on real LOL dataset images [own work]. (a) Input low-light image; (b) SmoothAdaptive Ensemble result; (c) Zero-DCE result; (d) Ground truth image.

The proposed method reduces underexposure while preserving texture structure, whereas the Zero-DCE output is visually cleaner in some regions but may lose fine local details. A systematic comparison of four different approaches to improving low-light images on fifteen test pairs from the LOL dataset was carried out. The first approach is represented by the developed SmoothAdaptive Ensemble method with a full adaptive weighting algorithm and double Gaussian smoothing. The second approach implements Blended Ensemble, which performs a simple unweighted averaging of the results of four base models without assessing local quality. The third approach uses Pyramid Ensemble, which processes images at three different scales and combines the results with weights of sixty percent for the original scale, thirty percent for half scale, and ten percent for quarter scale. The fourth approach is represented by the Zero-DCE model, which was trained on the training part of the LOL dataset for one hundred epochs with a batch size of four and a learning rate of one ten-thousandth.

The SmoothAdaptive Ensemble method demonstrated the highest PSNR among all the studied approaches, reaching a value of seventeen point ninety-one hundredths of a decibel. This result is fourteen point two tenths of a percent better than the Zero-DCE model, which showed a PSNR of fifteen point sixty-eight hundredths of a decibel. Blended Ensemble showed an intermediate result of sixteen point forty-six hundredths of a decibel, indicating the advantage of adaptive weighting over simple averaging. Pyramid Ensemble showed the lowest PSNR of fourteen point ninety-one hundredths of a decibel, which may be due to loss of detail when rescaling images multiple times.

According to the SSIM metric, the best result was shown by Pyramid Ensemble with a value of zero point seven hundred and forty-three thousandths, which indicates the effectiveness of multi-scale processing in

preserving the structural details of the image. Blended Ensemble achieved an SSIM of zero point seven hundred and sixteen thousandths. SmoothAdaptive Ensemble showed a value of zero point six hundred and seventy-eight thousandths, which is slightly lower than previous methods. The Zero-DCE model demonstrated an SSIM of zero point six hundred and forty-one thousandths, which is the lowest result among all methods.[10]

According to the Entropy metric, the developed SmoothAdaptive Ensemble achieved the highest value of seven point nineteen hundredths of a bit per pixel, which indicates the maximum information content and detail of the resulting images. Blended Ensemble showed six point eighty-four hundredths, Pyramid Ensemble six point thirty-eight hundredths, and Zero-DCE six point twenty-seven hundredths of a bit per pixel. This hierarchy of results is consistent with the PSNR scores and confirms the effectiveness of adaptive weighting in preserving visual information.

On the Average Gradient metric, which characterizes the sharpness of images, the SmoothAdaptive Ensemble also showed the best result of fifty-seven point thirty-four hundredths of one. Blended Ensemble achieved forty-three point eighty-six hundredths, Zero-DCE thirty-five point forty-eight hundredths, and Pyramid Ensemble only twenty-four point seventy-one hundredths of one. The high gradient of the SmoothAdaptive Ensemble indicates the effective restoration of sharp edges and textures in the enhanced images.

A critical difference between the classical ensembles and the Deep Learning approach is the processing speed. The Zero-DCE model demonstrated the fastest processing with a time of six hundred twenty-one milliseconds per image due to an efficient forward pass through a convolutional neural network on the GPU. SmoothAdaptive Ensemble requires six thousand seventy-three milliseconds, which is ten times slower. Blended Ensemble runs in five thousand three hundred thirty-three milliseconds, while Pyramid Ensemble is the slowest, with a time of six thousand nine hundred twenty-four milliseconds due to the need to process images at multiple scales.

V. CONCLUSIONS

Images captured under low-light conditions often suffer from (partially) poor visibility. Besides unsatisfactory lightings, multiple types of degradations, such as noise and color distortion due to the limited quality of cameras, hide in the dark. [11] This paper proposes and studies effective networks capable of producing brighter, clearer, and visually compelling images under diverse and challenging conditions.[12][13] The developed SmoothAdaptive Ensemble system combines four classical image processing algorithms through an adaptive weighting mechanism based on a local assessment of the quality of the results of each algorithm. The key

innovation of the method is the procedure of double Gaussian smoothing of quality maps and weights, which completely eliminates pixelation artifacts characteristic of previous block adaptive methods.

Experimental research on the standard LOL dataset demonstrated that the developed classical ensemble approach achieves a PSNR of seventeen point ninety one hundredths of a decibel, which is fourteen point two tenths of a percent higher than the result of the modern Deep Learning model Zero-DCE after one hundred training epochs. High values of the Entropy and Average Gradient metrics confirm the effectiveness of the method in restoring details and preserving the information content of images. At the same time, the method does not require a training stage on datasets, GPU calculations and large amounts of training data.[14]

Comparative analysis revealed a clear trade-off between the quality of improvement and processing speed. The classical ensemble approach provides a higher quality of detail restoration, full interpretability of the algorithm, and no need for training, but works ten times slower compared to optimized Deep Learning models. This defines different niches of practical application: classical ensembles are optimal for offline processing and systems without GPU, while Deep Learning approaches are preferable for real-time applications and mobile applications after appropriate training.

The practical applicability of the developed method has been confirmed for scenarios of offline processing of photo archives, professional photographic retouching, embedded systems without GPU and prototyping before developing specialized Deep Learning solutions. The full interpretability of the method makes it especially valuable in applications where understanding and explanation of decisions made in image processing is required.

Similar insights into the importance of robust and interpretable image processing pipelines have been demonstrated in the context of road accident detection algorithms for modern machine vision systems, where the selection of suitable models and features significantly affects reliability. [15]

The results demonstrate that classical image processing methods remain competitive and practically applicable when properly combined with adaptive ensemble approaches. Further development of the method through specialized denoising, automatic parameter tuning, and GPU optimization can further expand the scope of its effective application.

REFERENCES

- [1] Y. Wang, W. Xie, H. Liu "Low-light image enhancement based on deep learning: a survey", *Optical Engineering*, Vol. 61, Issue 4, 040901 (April 2022). <https://doi.org/10.1117/1.OE.61.4.040901>
- [2] S. Bielytsov, I. Ruban, K. Smelyakov, and D. Sumtsov, "Network technology for transmission of visual information," in *Selected Papers of the XVIII Int. Sci.-Practical Conf. "Information Technologies and Security" (ITS 2018)*, Kyiv, Ukraine, Nov. 27,

- 2018, CEUR Workshop Proceedings, vol. 2318, 2018, pp. 160–175. [Online]. Available: <https://ceur-ws.org/Vol-2318/>
- [3] M. Galar, A. Fernández, E. Barrenechea, H. Bustince, F. Herrera “An overview of ensemble methods for binary classifiers in multi-class problems: Experimental study on one-vs-one and one-vs-all schemes” Volume 44, Issue 8, August 2011, Pages 1761-1776, <https://doi.org/10.1016/j.patcog.2011.01.017>
- [4] F. Zavala “Histogram equalization CLAHE algorithm “, Mar 17, 2025. Available: <https://medium.com/imagecraft/histogram-equalization-clahe-algorithm-8841d402fc76>
- [5] J. Guo, J. Ma, Á. F. García-Fernández, Y. Zhang, H. Liang, “A survey on image enhancement for Low-light images”, <https://doi.org/10.1016/j.heliyon.2023.e14558>
- [6] S. Soni, P. Singh, A. A Wao, “Review of gamma correction techniques in digital imaging “, DOI : <https://doi.org/10.29121/shodhkosh.v5.i5.2024.1902>
- [7] S. Saleh Al-amri “Contrast Stretching Enhancement in Remote Sensing Image”, Available: https://bioinfopublication.org/files/articles/1_1_2_BIOINFO_SN.pdf
- [8] C. Guo, C. Li, J. Guo, C. Change Loy, J. Hou, S. Kwong, R. Cong “Learning to Enhance Low-Light Image via Zero-Reference Deep Curve Estimation”, <https://doi.org/10.48550/arXiv.2001.06826>
- [9] A. Sarala, C. Vinoth kumar “A cutting-edge ensemble model for enhanced underwater image restoration and quality improvement”, https://doi.org/10.1038/s41598-025-96832-8?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
- [10] C. Guo, C. Li, J. Guo, C. Change Loy, J. Hou, S. Kwong, R. Cong “Zero-Reference Deep Curve Estimation for Low-Light Image Enhancement”, <https://doi.org/10.48550/arXiv.2001.06826>
- [11] C. Wei, W. Wang, W. Yang, J. Liu “Deep Retinex Decomposition for Low-Light Enhancement”, 14 Aug 2018, <https://doi.org/10.48550/arXiv.1808.04560>
- [12] Y. Zhang, J. Zhang, X. Guo “Kindling the Darkness: A Practical Low-light Image Enhancer”, October 2019, <https://doi.org/10.1145/3343031.3350926>
- [13] X. Liu, Z. Wu, F.-Alexandru Vasluianu “NTIRE 2025 Challenge on Low Light Image Enhancement: Methods and Results”, 15 Oct 2025, <https://doi.org/10.48550/arXiv.2510.13670>
- [14] A. Daemdoost, A. Shahbahrani, H. Noorpoor, N. Esmi, R. Hassanpour “GPU optimizations to accelerate an image enhancement algorithm” Jun-2025, https://doi.org/10.1007/s11227-025-07447-9?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
- [15] O. Byzkrovnyi, L. Savulioniene, K. Smelyakov, P. Sakalys, and A. Chupryna, "Comparison of Potential Road Accident Detection Algorithms for Modern Machine Vision System," Vide. Tehnologija. Resursi – Environment, Technology, Resources, vol. 3, pp. 50–55, 2023, <https://doi.org/10.17770/etr2023vol3.7299>

Assessment of the Digital Maturity of ESG Reporting in the Context of Digitalization

Kiril Luchkov

Department of Economics, Industrial
Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Abstract — This study examines the digitization of ESG reporting through the lens of its digital maturity. The Digital ESG Reporting Maturity Index (DERMI) was developed for the quantitative assessment of the level of digitalization of ESG reporting. It is based on a set of measurable indicators combined into an index that covers five dimensions: format and machine readability, structuring according to the ESRS, degree of quantitative disclosure, presence of targets, and mechanisms for traceability and external assurance. The proposed index was tested on a sample of ESG reports to determine levels of digital maturity. The results indicate a moderate level of digital maturity, with significant variability among individual observations. It is found that digitalization is not limited to the implementation of technological solutions but is linked to the degree of data structuring, quantitative disclosure, and the presence of control and external assurance mechanisms.

Keywords — ESG reporting, digitization, digital maturity, sustainable development

I. INTRODUCTION

Over the past few years, the digitization of ESG reporting has transformed the way sustainability-related information is created, structured, and used [1]. Earlier studies on corporate social responsibility reporting have likewise emphasized that the quality of sustainability disclosure strongly depends on the design and reliability of supporting information systems [2]. The introduction of the European Sustainability Reporting Standards (ESRS) sets specific requirements for the content and organization of data, including its comparability and machine-readability [3]. In this context, digitization is not merely a matter of choosing a format [4]. It implies a certain level of structuring and internal consistency of information. This raises the question of measuring the digital maturity of ESG reporting, which is determined by technological solutions, data structuring, and process management [5], [6]. Recent reviews of artificial intelligence in digital infrastructures further show that data structuring, interoperability and

automated analytics are becoming central elements of modern reporting and control systems [7].

Existing studies primarily examine the regulatory framework and technological aspects of ESG reporting [8], [9]. Meanwhile, the quantitative measurement of its digital maturity remains in the background. There is a lack of tools that would allow for a systematic assessment and comparison of ESG reports across different companies [10], [11].

This study addresses this gap by developing a methodology for assessing the digital maturity of ESG reporting. The methodology is based on clearly defined indicators and leads to the construction of an index that enables quantitative measurement and comparative analysis of ESG reports.

II. THEORETICAL AND REGULATORY FOUNDATIONS OF THE DIGITALIZATION OF ESG REPORTING

The digitalization of ESG reporting should not be seen as a secondary technical layer, but as a change in the very architecture of corporate reporting. If the traditional model of non-financial reporting was oriented mainly towards the presentation of textual disclosures, the modern logic of sustainable reporting requires that data be structured in a way that allows digital processing, validation, and comparison.

The digital transformation of ESG reporting in the European Union is associated with the Corporate Sustainability Reporting Directive (CSRD). The European Commission emphasizes that the CSRD introduces more detailed requirements regarding sustainable reporting, which gradually cover different groups of enterprises. The ESRS specify the content and logic of these disclosures. For example, they address the general and thematic requirements for the presentation of information on impacts, risks, and opportunities [12].

The role of the European Securities and Markets Authority (ESMA) and the European Single Electronic Format (ESEF) in the digitalization process is particularly important. ESMA sees the digitalization of sustainability

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.169>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

reporting within the ESEF framework as part of a broader electronic reporting infrastructure. This means that ESG reporting is gradually integrated into existing digital corporate disclosure mechanisms. It does not develop as a separate and disconnected format. Such integration creates the prerequisites for higher comparability, controllability, and regulatory traceability of sustainable disclosures [13].

A significant feature of the current period is the dynamics of the regulatory framework itself. In 2025, the European Commission took action to simplify the rules for sustainability reporting through the Omnibus I package and the related changes to the first set of ESRS. As of spring 2026, the institutional process of revising the standards is ongoing, with the European Commission declaring its intention to adopt a delegated act with simplified ESRS before summer 2026 [14]. Therefore, the analysis of digitalization should take into account not only the current rules, but also the regime of their gradual improvement.

The international context complements this picture. The IFRS Sustainability Disclosure Taxonomy aims to transform sustainability-related disclosures into machine-readable information. This shows that the European process is not isolated, but is part of a broader global trend towards the digital structuring of sustainability reporting [15].

III. MATERIALS AND METHODS

To assess the level of digital maturity in ESG reporting, a quantitative methodology based on a set of measurable indicators has been developed and applied. Indicator-based approaches are also widely used for evaluating the effectiveness of enterprise information-system implementation and digital organizational readiness [16]. The methodology is not intended to produce representative generalizations for the aggregate of companies across various economic sectors. Its purpose is to determine to what extent the digitalization of ESG reporting can be assessed using a set of indicators. On this basis, a comparative assessment index is constructed. Comparable indicator-based approaches have also been used to assess the effectiveness of digital platforms and technology-enabled organizational systems [17].

The unit of analysis is the individual ESG report. The study covers 12 observations, designated as R1–R12. The sample was formed through targeted selection to ensure variability across key characteristics of ESG reporting. The approach is analytical in nature and is not aimed at achieving statistical representativeness.

The number of ESRS thematic areas covered is used as an empirical indicator of the degree to which ESG reporting is structured in accordance with ESRS requirements. The indicator reflects the extent to which the ESG report aligns thematically with the ESRS disclosure framework, without directly measuring the quality of that alignment.

The assessment is conducted using a proprietary index for the digital maturity of ESG reporting (Digital ESG Reporting Maturity Index, DERMI), which includes five components:

- (1) format and degree of machine readability;
- (2) structuring in accordance with the requirements of the ESRS;

(3) proportion of quantitatively presented ESG indicators;

(4) presence of targets with a baseline value and a timeline; and

(5) traceability and external assurance of the information.

The proportion of quantitatively reported KPIs is calculated as the ratio of quantitatively disclosed ESG indicators to the total number of identified indicators within the relevant ESG report. Indicators presented solely in a descriptive or qualitative form are not treated as quantitatively disclosed. The identification of indicators was based on the structure of ESG disclosures and the relevant thematic areas under the ESRS.

Each component is assessed on a scale of 0 to 2 points, and the total index score ranges from 0 to 10 points. The individual components and evaluation criteria are presented in Table 1.

TABLE 1 COMPONENTS OF THE DERMI INDEX

Component	Evaluation criterion	Scale
Format and machine readability	Assessing the suitability of the ESG report for digital processing	0 = static document format; 1 = structured digital representation; 2 = machine-readable format (iXBRL/XBRL)
Structuring according to ESRS	The degree of thematic structuring and alignment of the ESG report with ESRS disclosure requirements is assessed.	0 = low; 1 = partial; 2 = high
Quantitative coverage of KPIs	The proportion of indicators presented in quantitative form is assessed.	0 = below 50%; 1 = 50–69%; 2 = 70% and above
Objectives, baseline and deadline	Assesses whether the ESG report contains measurable objectives, baseline and time horizon.	0 = absent; 1 = partial; 2 = all three present
Traceability and external assurance	The degree of traceability of ESG disclosures, including source referencing, methodological transparency and external assurance availability, is assessed.	0 = both missing; 1 = only one element is present; 2 = both are present

Source: Authors' own research.

Traceability refers to the possibility of linking ESG disclosures to identifiable data sources, methodological explanations and supporting documentation. The assessment considers the presence of internal referencing mechanisms, transparency of disclosure methodology and the verifiability of reported information.

Formally, the index can be expressed as follows:

$$\text{DERMI} = \text{FR} + \text{ESRS} + \text{KPI} + \text{TG} + \text{CT},$$

where:

- (1) FR is the component for format and machine readability;
- (2) ESRS is the component for thematic structuring, KPI is the component for quantitative coverage,
- (3) TG is the component for goal setting, and
- (4) CT is the component for traceability and external assurance.

For the purposes of interpreting the results, three levels of digital maturity were used: low (0–3 points), medium (4–6 points), and high (7–10 points). The thresholds were analytically defined in order to distinguish between limited, transitional and advanced levels of ESG reporting digital maturity based on the cumulative fulfillment of DERMI components.

IV. RESULTS

Table 2 presents information on the observations included in the sample. It includes selected ESG reporting indicators and the corresponding DERMI index values. The table serves as an empirical basis for the subsequent comparative analysis of digital maturity.

TABLE 2 ESG REPORTS ANALYZED AND DERMI INDEX VALUES

ID	Volume (pages)	Number of ESRS thematic areas covered	KPIs (%)	External assurance	DERMI
R1	120	10	78	Yes	10
R2	110	9	74	Yes	10
R3	98	8	72	Yes	9
R4	95	8	69	No	7
R5	87	7	66	No	7
R6	82	7	61	Yes	7
R7	76	6	58	No	5
R8	74	6	54	Yes	5
R9	69	5	47	No	3
R10	63	4	45	Yes	2
R11	68	5	49	No	1
R12	65	4	40	No	1

Note: 1/ Sort by DERMI (descending).

2/ The KPI share (%) is calculated as the ratio between the quantified indicators and the total number of indicators identified in the report.

Source: Authors' own research.

The results indicate a moderate average level of digital maturity, combined with significant internal variation. The average DERMI index score is 5.58 out of a possible 10 points. This indicates that the transition to more mature digital ESG reporting is visible but not yet uniform. Six of the twelve observations show high digital maturity, two show moderate maturity, and four show low maturity.

For a more detailed description of the sample, Table 3 presents summary statistics for each variable. The data show a moderate volume of reports and an average level of coverage of ESRS thematic areas and the quantitative

indicators presented. There is significant variability among the individual observations.

TABLE 3 SUMMARY STATISTICS

Indicator	Average value	Median	Standard deviation	Minimum value	Maximum value
Report volume (pages)	83.9	79.0	18.5	63	120
Number of ESRS thematic areas covered	6.6	6.5	1.9	4	10
Quantified KPIs (%)	59.4	59.5	12.6	40	78
DERMI Index (0-10)	5.6	6.0	3.3	1	10

Source: Authors' own research.

The average length of the ESG reports in the sample is 83.92 pages, the average number of ESRS thematic areas covered is 6.58, and the average proportion of KPIs presented quantitatively is 59.42%. Reports with external assurance achieve an average DERMI score of 7.17 points, while reports without assurance achieve an average score of 4.00 points. The observed difference should be interpreted with due caution given the limited sample size. The study found that digital maturity is not determined solely by technological characteristics. It is associated with a higher degree of data structuring, quantitative disclosure, and external assurance.

V. DISCUSSION

Empirical results show that higher DERMI scores are associated with more robust quantitative disclosure practices. These scores are also linked to broader thematic alignment with ESRS requirements and the presence of external assurance mechanisms. In contrast, reports with lower DERMI scores are characterized by a fragmented structure of ESG information. They also exhibit a lower proportion of quantitative indicators and less pronounced traceability characteristics. These findings are broadly consistent with previous studies emphasizing the importance of structured ESG data governance, interoperability, and assurance mechanisms in digitally mature reporting systems [18], [19].

The overall analysis shows that the digitalization of ESG reporting should not be presented as a quick technological fix or a purely administrative burden. Rather, it should be perceived as a process of institutional and organizational maturation, in which regulatory requirements, taxonomies, digital tools, and internal processes evolve simultaneously. In ESG practice, there are opportunities to increase the transparency and comparability of information. At the same time, there are also challenges in the early implementation of ESG reporting requirements.

It has been found that the digital format does not guarantee the quality of ESG reporting. It can make the

information easier to use, but only if this information is the result of structured internal processes. Otherwise, digitalization tends to increase the visibility of already existing organizational weaknesses. Therefore, the real subject of digital ESG reporting is not just the published file, but the data architecture behind it [10].

From this perspective, sustainable progress in this area will depend not so much on the quantity of technological solutions, but on the ability of enterprises to build consistent data management systems, internal controls, proportionate processes and interoperable formats [9], [20]. This turns the digitalization of ESG reporting into an intersection between regulation, accounting logic, information management and sustainability-related policies.

VI. CONCLUSIONS

Based on the analysis, it can be concluded that the digitalization of ESG reporting is a natural stage in the development of corporate reporting. This process reflects a clear trend towards standardization, digital structuring and increased usability of sustainable information. The results show that machine-readable ESG reporting can help improve the comparability, traceability, and analytical usability of sustainability disclosures.

The results of the study indicate that the positive effect of digitalization is not guaranteed. It was found that it depends on the quality of primary data, the maturity of internal processes, and the clear distribution of responsibilities. Of additional importance is the ability of enterprises to function in a changing regulatory environment. To ensure transparency and comparability of data, the use of digital tools is recommended, provided that they are supported by a reliable organizational framework that includes processes, responsibilities, and control mechanisms.

From a practical point of view, several key recommendations can be formulated. First, companies should start structuring ESG data at the stage of its collection, and not only when preparing the final report. Second, it is necessary to prefer open and standardized formats and avoid unnecessary dependence on difficult-to-portable solutions. Third, it is necessary to build a clear internal system that guarantees data ownership, management, verification and control. Fourth, for smaller companies, proportionate tools and templates should be applied that reduce complexity without compromising quality.

VII. ACKNOWLEDGEMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

- [1] Abhayawansa, S., Adams, C., Busulwa, R., & Shying, M. (2025). *The Digital Transformation of Sustainability Reporting: How Digital Technologies are Reshaping Sustainability Accounting, Data, and Disclosure*. Routledge. <https://doi.org/10.4324/9781032637938>
- [2] Stoyanov, P., Anguelov, K. (2025). Corporate Social Responsibility Reporting: Information System Requirements, 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, doi: [10.1109/COMSCI67172.2025.11225210](https://doi.org/10.1109/COMSCI67172.2025.11225210).
- [3] European Commission. (2022). Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 as regards corporate sustainability reporting. Official Journal of the European Union, L 322, 15–80. <https://data.europa.eu/eli/dir/2022/2464/oj>
- [4] Brenner, B. (2018). Transformative Sustainable Business Models in the Light of the Digital Imperative - A Global Business Economics Perspective. Sustainability, 10(12), 4428. <https://doi.org/10.3390/su10124428>
- [5] Christensen, H. B., Hail, L., & Leuz, C. (2021). Mandatory CSR and sustainability reporting: economic analysis and literature review. Review of Accounting Studies, 26, 1176–1248. <https://doi.org/10.1007/s11142-021-09609-5>
- [6] Yu, J., & Moon, T. (2021). Impact of Digital Strategic Orientation on Organizational Performance through Digital Competence. Sustainability, 13(17), 9766. <https://doi.org/10.3390/su13179766>
- [7] Zinoviev, V., Koeva, D., Tsankov, P., Kutkarska, R. (2026). Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. Energies, 19, 1250. <https://doi.org/10.3390/en19051250>
- [8] Alles, M. G. (2015). Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession. Accounting Horizons, 29(2), 439–449. <https://doi.org/10.2308/acch-51067>
- [9] Lai, A., Melloni, G., & Stacchezzini, R. (2016). Corporate Sustainable Development: is 'Integrated Reporting' a Legitimation Strategy? Business Strategy and the Environment, 25, 165–177. <https://doi.org/10.1002/bse.1863>
- [10] Appelbaum, D., Kogan, A., Vasharhelyi, M., & Yan, Z. (2017). Impact of business analytics and enterprise systems on managerial accounting. International Journal of Accounting Information Systems, 25, 29–44. <https://doi.org/10.1016/j.accinf.2017.03.003>
- [11] Lock, I., & Seele, P. (2015). Analyzing Sector-Specific CSR Reporting: Social and Environmental Disclosure to Investors in the Chemicals and Banking and Insurance Industry. Corporate Social Responsibility and Environmental Management, 22, 113–128. <https://doi.org/10.1002/csr.1338>
- [12] European Commission. (2024). Corporate sustainability reporting. https://finance.ec.europa.eu/financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en
- [13] European Securities and Markets Authority. (2024). Electronic reporting. <https://www.esma.europa.eu/issuers-disclosure/electronic-reporting>
- [14] European Securities and Markets Authority. (2026). Opinion on revised ESRS. https://www.esma.europa.eu/sites/default/files/2026-02/ESMA32-846262651-5440_Opinion_on_revised_ESRS.pdf
- [15] IFRS Foundation. (2024). IFRS Sustainability Disclosure Taxonomy. <https://www.ifrs.org/issued-standards/ifrs-sustainability-taxonomy/>
- [16] K. Anguelov, Indicators for the Effectiveness and Efficiency of the Implementation of an Enterprise Resource Planning System, 2021 12th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 2021, pp. 1-4, doi: [10.1109/ELECTRONICA52725.2021.9513729](https://doi.org/10.1109/ELECTRONICA52725.2021.9513729).
- [17] M. Angelova, Indicators for Effectiveness and Efficiency of E-Platforms for Business Meetings, 2020 III International Conference on High Technology for Sustainable Development (HiTech), Sofia, Bulgaria, 2020, pp. 1-4, doi: [10.1109/HiTech51434.2020.9364000](https://doi.org/10.1109/HiTech51434.2020.9364000).

- [18] Perdana, A., Robb, A., & Rohde, F. (2015). An Integrative Review and Synthesis of XBRL Research in Academic Journals. *Journal of Information Systems*, 29(1), 115–153. <https://doi.org/10.2308/isis-50884>
- [19] Wu, S., & Li, Y. (2023). A Study on the Impact of Digital Transformation on Corporate ESG Performance: The Mediating Role of Green Innovation. *Sustainability*, 15(8), 6568. <https://doi.org/10.3390/su15086568>
- [20] Yang, Y., & Han, J. (2023). Digital transformation, financing constraints, and corporate environmental, social, and governance performance. *Corporate Social Responsibility and Environmental Management*, 30(6), 3189–3202. <https://doi.org/10.1002/csr.2546>

Computer Science Students' Perspectives on Incorporating Digital Storytelling for Developing Critical Thinking Skills in English Classroom

Oleksandr Malykhin
Department of Didactics
Institute of Pedagogy of NAES of
Ukraine
Kyiv, Ukraine
orcid.org/0000-0001-6042-6298

Nataliia Aristova
Department of International
Relations and Research Cooperation
Institute of Pedagogy of NAES of
Ukraine
Kyiv, Ukraine
orcid.org/0000-0002-0943-8039

Liudmyla Dybkova
Department of Informatics and
Systemology
Kyiv National Economic University
named after Vadym Hetman
Kyiv, Ukraine
orcid.org/0000-0002-3920-118X

Abstract—In the era of rapid technological advancement, access to digital opportunities makes it possible to prepare students for the jobs of the future and have a positive influence on the development of their future-proof skills, which will be of paramount value. Amid unpredictable changes in the labor market, critical thinking skills are becoming increasingly strategic and enabling labor market entrants to think independently and make informed decisions. Although numerous studies suggest that digital technologies can enhance students' engagement and motivation, the current academic literature lacks research that captures students' perspectives on developing critical thinking skills through digital storytelling. To address this gap, the study aims to investigate students' perspectives on incorporating digital storytelling for developing critical thinking skills in the English classroom. To achieve this aim, the researchers developed a questionnaire containing both open- and closed-ended questions and surveyed 397 computer science undergraduate students from two Ukrainian universities. The findings demonstrate that all students surveyed consider digital storytelling an effective way to develop their critical thinking skills, and digital tools are convenient for creating, visualizing and presenting ideas. To draw well-founded conclusions, the researchers use both qualitative and quantitative data analysis. This study is limited to computer science undergraduate students studying English.

Keywords—computer science students, critical thinking skills, digital storytelling, digital technologies.

I. INTRODUCTION

As all aspects of modern society become increasingly digitized, there is a growing need not only for professionals with in-depth hard skills but also for those capable of innovative and critical thinking [1]. To keep pace with rapid changes and remain at the forefront of the Tech

industry, computer science specialists already working in the market must not only adapt and generate new ideas but also continuously improve their professional competencies [2]. Changing labor market needs mean that the demand for such specialists capable of creating new technologies and products is driving new requirements for computer science students' training, particularly in developing critical thinking as the foundation for innovative, unconventional solutions.

The accelerated digitization of higher education is driving the modernization of traditional approaches, teaching techniques and methods through the use of digital technologies, helping ensure the accessibility and quality of education for today's students [3]. Considering the level of advancement of digital technologies and their accessibility for a wide range of users, it is obvious that they are becoming increasingly popular among both teachers and students. Given that each type of digital technology has its own advantages and disadvantages, teachers should have a range of user-friendly technologies at their disposal that facilitate the effective organization of students' educational activities. Currently, one of the innovative teaching methods that harmoniously combines classic principles of narrative construction with digital ways of presenting, appealing to students growing up in the digital world, is digital storytelling [3; 4; 5].

The literature shows that an increasing number of modern researchers are seeking to define and formulate the "digital storytelling" concept and to demonstrate, with supporting evidence, the benefits of applying digital storytelling in the educational context. For instance, according to Robin, digital storytelling is an "art of telling stories with a mixture of digital media, including text, pictures, recorded audio narration, music, and video" [6, p. 18]. We favour Robin's idea that digital storytelling is not

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.140>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

only about boosting students' communication skills, creativity, and motivation and showing a thorough understanding of topics they study, but it is also about giving them "a voice to share their ideas and feelings with others" [6, p. 19].

Cai expresses a similar idea concerning the definition of the "digital storytelling" concept [7]. The scientist defines it as a tool that "combines traditional narrative techniques with modern digital technology to create a new and highly interactive narrative experience [7, p. 91]. In the context of our research, the most valuable is the idea expressed by Cai that the use of digital storytelling in the classroom helps improve students' motivation and enhance classroom interaction, on the one hand, and, on the other hand, it enables the enhancement of students' overall experience, which leads to a deeper understanding of educational content [7].

Alismail considers digital storytelling as a tool that "combines researching, creating, analyzing, and combining visual images with written text, which is considered a positive style in teaching" [8, p. 127]. The researcher contends that to enhance students' motivation to improve their learning and performance, teachers have to use this kind of activity in their classrooms. However, believing that digital storytelling is effective in developing students' higher-order thinking skills and motivation, Alismail states that further research is required in this field [8].

Parole et al. [9] propose their own definition of the "educational digital storytelling" concept and detail the benefits of creating digital stories in the classroom. The team of researchers defines it as "facilitated production of a short digital story in an educational community setting that should contain a mixture of digital media, including text, recorded audio narration, pictures, music, and video" [9, p. 119]. They also view digital storytelling as an efficient tool for facilitating students' reflection on and pursuit of a meaningful life shaped by their interests and motives.

In their study Austen, Jones and Wawera provide a definition of "digital stories" concept which they regard as "a collection of still images with accompanying audio or textual narration, and used as data in student voice research within higher education" [10, p. 27].

Gürsoy, who conducted research to examine the influence of digital storytelling on the development of 21st-century skills, concludes that digital storytelling is effective in improving a wide range of skills [11]. The researcher groups these skills into three categories: learning and innovation; information, media, and technology; and life and professional skills [11, p. 105]. Interestingly, the life and professional skills category included skills such as taking responsibility, critical thinking, and planning. In research conducted by Gürsoy, respondents stated that providing feedback on digital stories enabled them to acquire a critical perspective, which is an inseparable part of critical thinking [11].

Of particular interest to our research is a definition of "digital storytelling" concept formulated by Yang, & Wu

[1]. The researchers believe it is "a promising transformative technology-supported approach for enhancing learning, including subject matter content acquisition, critical thinking skills, motivation, and information literacy" [1, p. 340].

Although numerous studies suggest that digital technologies can enhance students' engagement and motivation [12; 13; 14; 15; 16], the current academic literature lacks research that captures students' perspectives on developing critical thinking skills through digital storytelling. To address this gap, the study aims to investigate students' perspectives on incorporating digital storytelling for developing critical thinking skills in the English language classroom.

II. MATERIALS AND METHODS

For the investigation, the researchers developed a questionnaire containing both open- and closed-ended questions. To characterize the student sample, the researchers included several demographic questions about professional activity and participation in additional career-oriented courses. Among the respondents, 48.11% (191 computer science students) balance their studies and work. 61.96% of respondents (246 computer science students) experience participating in additional career-oriented courses.

As part of data collection process, the questionnaire contains two closed-ended questions:

Q 1. Do you believe that digital storytelling is useful for developing critical thinking skills?

Q 2. Is digital storytelling more effective for developing critical thinking skills than traditional methods like textbooks and lectures?

The questionnaire contains two closed-ended questions aimed at rating on a 5-point Likert scale (ranging from 1 – "strongly disagree (SD)", 2 – "disagree (D)", 3 – "neutral (N)", 4 – "agree (A)", 5 – "strongly agree (SA)"):

Q 3. To what extent do you agree that digital storytelling helps develop critical thinking skills?

Q 4. To what extent do you agree that digital storytelling should be a part of your learning in the English language classroom?

The questionnaire contains three open-ended questions:

Q 5. Which skills, in addition to critical thinking, do you develop most by making digital stories?

Q 6. Which aspects of your critical thinking have improved as a result of participating in digital storytelling?

Q 7. What challenges do you face while creating digital stories?

In this study, English is selected as the survey discipline because it is an obligatory component of the computer science students' curriculum and it incorporates various innovative teaching and learning methods including digital storytelling.

To provide a clearer understanding of digital storytelling exercises, an example is given in Table 1.

TABLE 1 AN EXAMPLE OF DIGITAL STORYTELLING EXERCISE

Topic	Blended Learning vs Traditional Learning: Benefits and Challenges
Objective	To develop students' ability to analyze information regarding the benefits and challenges of blended and traditional learning, critically assess the information studied, formulate their own positions and argue them convincingly, draw and justify their own conclusions
Instructions	First, write a short story in English (150-200 words) based on the analysis of modern scientists' papers on the benefits and challenges of blended and traditional learning. The story should include an introduction, 2-3 main arguments, and a conclusion. Second, prepare images, photos, or drawings (you may use your own or find free images on the Internet). If using photos/images/drawings from the Internet, please provide proper source references. Third, record yourself narrating the digital story in English.
Digital tools	Use Canva or Google Slides (or any other digital tool) to create and present the digital story
Assessment Criteria	Be ready that the groupmates will assess the digital story using the following assessment criteria: - English language proficiency (grammatical accuracy and appropriate vocabulary usage); - creativity and originality; - well-balanced presentation structure; - quality of arguments and examples; - effective integration of multimedia elements; - ability to answer question after presenting the digital story

The survey lasted three months, from September to November 2025. The sample comprised 397 computer science undergraduate students from two Ukrainian universities, namely, Kyiv National University of Technologies and Design and Kyiv National Economic University named after Vadym Hetman.

To ensure a comprehensive analysis, this study adopted a mixed-methods approach.

III. RESULTS AND DISCUSSION

The information collected from Q 1 shows that 329 respondents (82.87%) believe that digital storytelling is useful for developing critical thinking skills (Fig. 1). The survey results show that there are no negative responses from respondents. At the same time 68 respondents (17.13%) find it difficult to answer this question.

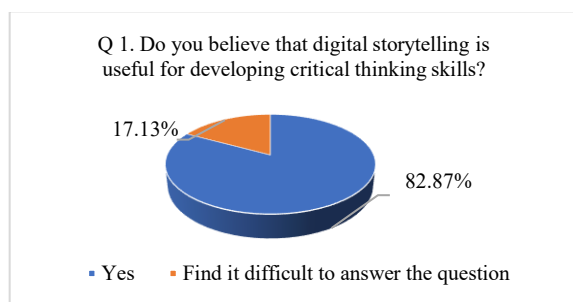


Fig. 1. The data obtained from respondents' answers to Question 1.

Replying to Q 2 "Is digital storytelling more effective for developing critical thinking skills than traditional methods like textbooks and lectures?", the survey results indicate the respondents' responses are predominantly positive – 341 respondents (85.89%). The responses received show a generally positive trend among respondents. These responses indicate that computer science students perceive this innovative teaching and learning method as effective for developing their critical thinking skills. 36 respondents (9.07%) find it difficult to answer the question. Only 20 respondents (5.04%) express a negative attitude (Fig. 2).

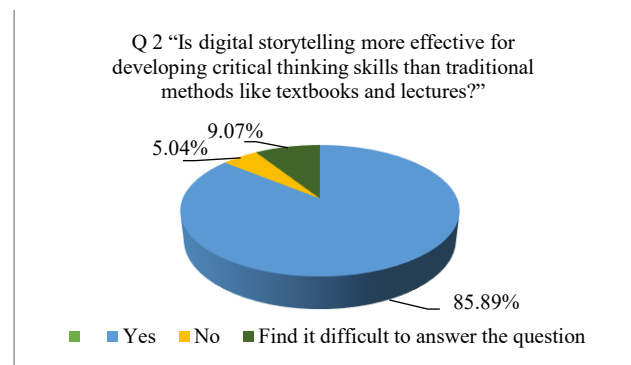


Fig. 2. The data obtained from respondents' answers to Question 2.

Q 3 is aimed to find out to what extent respondents agree that digital storytelling helps develop critical thinking skills. The results obtained are given in Table 2.

TABLE 2 RESPONDENTS' LEVEL OF AGREEMENT REGARDING EFFECTIVENESS OF DIGITAL STORYTELLING IN DEVELOPING CRITICAL THINKING SKILLS

Question 3	Variables				
	SD (1)	D (2)	N (3)	A (4)	SA (5)
To what extent do you agree that digital storytelling helps develop critical thinking skills?	16	39	64	155	123

Source (own study)

The table data demonstrate that only 4.03% of respondents strongly disagree with the view that digital storytelling helps develop critical thinking skills. In their turn, only 9.82% of respondents disagree with this view. 16.12% of respondents take a neutral stance. 39.04% of respondents agree and 30.98% of respondents strongly agree that digital storytelling helps develop critical thinking skills. The results obtained indicate the predominance of positive responses ($M \approx 3.88$, $SD \approx 1.06$, $Mdn=4$, $SE \approx 0.053$). The researchers use Student's t-distribution to assess whether the mean ($M \approx 3.88$) differs significantly from the neutral value ($t(396) \approx 16.41$, $p \approx 0.001$). We can infer that the respondents consider digital storytelling effective for developing critical thinking skills, as supported by both the distribution of responses and statistical analysis.

Table 3 presents the results concerning question 4 aimed at finding out the level of agreement among respondents on the idea that digital storytelling should be a part of their learning in the English language classroom.

TABLE 3 RESPONDENTS' LEVEL OF AGREEMENT REGARDING THE IDEA THAT DIGITAL STORYTELLING SHOULD BE A PART OF THEIR LEARNING IN THE ENGLISH LANGUAGE CLASSROOM

Question 3	Variables				
	SD (1)	D (2)	N (3)	A (4)	SA (5)
To what extent do you agree that digital storytelling should be a part of your learning in the English language classroom?	12	34	61	159	131

Source (own study)

The findings show that 3.02% of respondents strongly disagree and 8.56% disagree that digital storytelling should be part of their learning in the English language classroom. 15.37% of respondents express a neutral position. On the contrary, 40.05% of respondents agree, and 33.00% of respondents agree strongly with the suggested idea. The results obtained indicate the predominance of positive responses ($M \approx 3.91$, $SD \approx 1.039$, $Mdn = 4$, $SE \approx 0.052$).

By asking Q 5, the researchers imply they want to find out which skills, in addition to critical thinking, respondents think develop most when making digital stories. The analysis of respondents' responses enables the selection of the following categories: Category 1 – creativity and imagination; Category 2 – writing skills; Category 3 – emotional intelligence; Category 4 – communicative skills and confidence; Category 5 – digital skills; Category 6 – creative thinking and ability to structure ideas; Category 7 – visual literacy; Category 8 – time management skills; Category 9 – English language skills (Table 4).

TABLE 4 SKILLS THAT ARE DEVELOPED IN ADDITION TO CRITICAL THINKING WHILE USING DIGITAL STORYTELLING

Category	Responses	
	N	%
Creativity and imagination	197	49.62
Writing skills	194	48.87
Emotional intelligence	99	24.94
Communicative skills and ability to express ideas calmly	190	47.86
Digital skills	230	57.93
Ability to structure ideas	130	32.75
Visual literacy	95	23.93
Time management skills	32	8.06

Category	Responses	
	N	%
English language skills	68	17.19

Source (own study)

The findings suggest that respondents believe that along with developing critical thinking skills digital storytelling is effective in improving respondents' creativity and imagination (49.62%), writing skills (48.87%), emotional intelligence (24.94%), communicative skills and ability to express ideas calmly (47.86%), digital skills (57.93%), ability to structure ideas (32.75%), visual literacy (23.93%), time management skills (8.06%), English language skills (17.19%). These findings help us make an assumption that respondents view digital storytelling as a comprehensive teaching and learning method or process that positively influences the development of a range of creative, communicative, and technical skills, rather than reducing it to critical thinking skills alone.

The aim of Question 6 is to determine which aspects of critical thinking have improved as a result of participating in digital storytelling. The analysis of respondents' replies allows for the identification of the following categories: Category 1 – source analysis, Category 2 – structuring sought-after information, Category 3 – drawing well-founded conclusions, Category 4 – reflecting on work done, Category 5 – ability to create a basis for developing new solutions (Table 5).

TABLE 5 RESPONDENTS' VIEWS ON IMPROVING CRITICAL THINKING SKILLS

Category	Responses	
	N	%
Source analysis	157	39.55
Structuring sought-after information	218	54.91
Drawing well-founded conclusions	144	36.27
Reflecting on work done	229	57.68
Ability to see the situation from different perspectives	181	45.59

Source (own study)

The findings suggest that participation in the creation of digital stories helps computer students improve various aspects of critical thinking. Thus, for instance, 39.55% of respondents believe that their ability to analyze different sources improved greatly. In their replies, respondents mention that selecting information for creating interesting and informative digital stories requires a thorough study and analysis of websites, scientific papers, journals, etc. This way, they learn to analyze various sources of information. For 54.91% of respondents, participating in

digital storytelling means learning how to structure sought-after information. 36.27% of respondents point out that digital storytelling influenced the development of their ability to draw well-founded conclusions. It was interesting to find that 57.68% of respondents reported that digital storytelling improved their ability to reflect on their work. Presenting digital stories in lessons, participating in their assessment, sharing impressions with groupmates about the digital stories, and discussing the challenges they face while creating them positively influence the ability to reflect. 45.59% of respondents reported that digital storytelling helped them improve their ability to see the situation from a different perspective.

By including question 7 in the questionnaire, the researchers aim to identify the challenges computer science students face when creating digital stories. Analysis of the respondents' replies shows that although the respondents' opinions differ on the challenges they faced when creating digital content, they note that these challenges involved not only time management or technical skills but also critical thinking as well. Here are the excerpts for respondents' replies:

S15: *Creating digital stories can be time-consuming and technically distracting. Much depends on the topic, but sometimes you prioritize flashy visuals over the actual quality of your message. It usually happens when you do not have much time to analyze the necessary sources or structure the sought-after information. Now I think I take fact-checking more seriously.*

S29: *The main challenge I face is that it takes a lot of effort to design slides and fix technical issues. Sometimes I focus more on the design than on the content. ... At first, I didn't like such activities. I think it happened because I never checked the facts and used information which I could find quickly. I also didn't have enough skills concerning structuring the information and comparing different points of view....*

S76: *Although it makes me more confident and teaches me to draw well-founded conclusions and express myself properly, I have to admit that sometimes it is time-consuming. What I mean is that to create an informative digital story you have to find the necessary information. You spend much time on searching the Internet and when you find what you need, you have to spend more time analyzing and structuring this information. ... I like such activities, but sometimes it takes much time.*

S47: *I can mention several challenges, namely, time, technical obstacles, and visual image over content. Creation of digital stories can be time-consuming. It usually takes much longer to create a digital story than to write a simple essay (time). If you want to impress your teachers and groupmates by choosing innovative software, it also might cause some difficulties especially for those who don't have enough technical skills. If the Internet is slow, the whole process can be frustrating (technical obstacles). Sometimes you can focus so much on the music, images or effects that you forget about producing high-quality academic content (visual image over content).*

Recognizing these challenges helps acknowledge that developing students' critical thinking through digital storytelling requires appreciating their efforts and fostering a learning environment that provides full support for improving the skills they lack. Involving students in digital storytelling should be targeted at teaching them to use more effective learning strategies, namely time management, critical evaluation of information, critical processing of information, and conscious use of information.

IV. CONCLUSIONS

The study aimed to investigate computer science students' perspectives on incorporating digital storytelling for developing critical thinking skills in the English classroom. The findings obtained clearly demonstrate that computer science students are aware of the importance of critical thinking as a key competency for lifelong learning. The findings also reveal computer science students' general view of the need for a more practice-oriented, competency-based approach to education in higher education institutions, as well as the implementation of innovative methods to develop critical thinking skills in the English language classroom.

Based on the conducted research, we can conclude that the use of digital storytelling in the classroom makes it possible both to consider computer science students' abilities, their educational interests, needs, and their current level of knowledge in a particular discipline and to develop their cognitive abilities (including critical thinking skills as one of the key components of an individual's cognitive activity).

The conducted research highlights the following key findings: 1) the majority of computer science students consider digital storytelling an effective way to develop their critical thinking skills, and digital technologies convenient tools for creating, visualizing and presenting ideas; 2) present-day computer science students as representatives of generation growing up in the digital world perceive digital storytelling as more effective for developing critical thinking skills than traditional methods like textbooks and lectures; 3) digital storytelling is a comprehensive teaching and learning method or process that positively influences the development of a range of creative, communicative, and technical skills, rather than reducing it to critical thinking skills alone; 4) developing critical thinking skills through digital storytelling requires equipping students with effective learning strategies, namely time management, critical evaluation of information, critical processing of information, and conscious use of information.

V. STUDY LIMITATIONS

This study is limited to responses of computer science undergraduate students studying English as a compulsory discipline.

REFERENCES

- [1] Y.-T. C. Yang, W.-C. I. Wu, "Digital storytelling for enhancing student academic achievement, critical thinking, and learning motivation: A year-long experimental study," *Computers &*

- Education, 59, pp. 339-352, 2012.
<https://doi.org/10.1016/j.compedu.2011.12.012>
- [2] O. Malykhin, N. Aristova, and S. Melikova, "Soft Skills Development Strategies for Computer Engineering and Information Technologies Undergraduate Students Devised in the Process of Learning English", ETR, vol. 2, pp. 255-260, Jun. 2021. [Online]. Available: <https://archive-journals.rtu.lv/etr/article/view/4448> [Accessed Jan. 28, 2026], <https://doi.org/10.17770/etr2021vol2.6602>
- [3] L. Weiler, How Storytelling has changed in the digital age. World Economic Forum. Jan. 23, 2015.
https://www.weforum.org/stories/2015/01/how-storytelling-has-changed-in-the-digital-age/?gad_source=1&gad_campaignid=22228224717&gbraid=0AAAAoVy5F78OtcXXv46nK89p8IZ8KMuH&gclid=CjwKCAjwqazPBhALEiwAOuXqdNLxFAzEP7gZKrfDDL2LCNjx1HZ0o7XR9hmtOjciGCrB71ADean3KBoCxisQAvD_BwE
- [4] S. J. Kakungulu, "The Role of Digital Storytelling in Education: Enhancing Literacy and Communication Skills", Eurasian Experiment Journal of Scientific and Applied Research, vol. 5(2), pp. 36-39, 2024. [Online]. Available: https://www.researchgate.net/publication/383550648_The_Role_of_Digital_Storytelling_in_Education_Enhancing_Literacy_and_Communication_Skills [Accessed Feb. 16, 2026].
- [5] O. Malykhin, N. Aristova, and L. Dybkova, "Developing Computer Science Undergraduate Students' Communicative and Self-Expression Skills: Digital vs. Traditional Storytelling Methods," ETR, vol. 3, pp. 219-224, Jun. 2025, <https://doi.org/10.17770/etr2025vol3.8559>
- [6] B. R. Robin, "The Power of Digital Storytelling to Support Teaching and Learning," Digital Education Review, vol. 30, pp. 17-29, December 2016. [Online]. Available: <https://files.eric.ed.gov/fulltext/EJ1125504.pdf> [Accessed December 12, 2025].
- [7] M. Cai, "A Study and Application of Digital Storytelling in Digital Humanities Education," International Journal on New Developments in Education, vol. 6(10), pp. 91-100, 2024. [Online]. Available <https://francispress.com/papers/17327> [Accessed Dec. 14, 2025], <https://doi.org/10.25236/IJNDE.2024.061015>
- [8] H. H. Alismail, "Integrate Digital Storytelling in Education", Journal of Education and Practice, vol. 6, no. 9, 2015. [Online]. Available: <https://files.eric.ed.gov/fulltext/EJ1082416.pdf>. [Accessed: Feb. 25, 2026].
- [9] A. Parola, R. Di Fuccio, F. Somma, and J. Miglino, "Educational Digital Storytelling: Empowering Students to Shape Their Future", in Psychology, Learning, Technology. PLT 2022. Communications in Computer and Information Science, P. Limone, R. Di Fuccio, G. A. Toto, (eds), vol 1606, 2022, pp. 119-129. [Online]. Available: <https://rdcu.be/feE0Q> [Accessed Jan. 15, 2026].
- [10] G. Gürsoy, "Digital storytelling: Developing 21st century skills in science education," European Journal of Educational Research, 10(1), pp. 97-113, 2021. <https://doi.org/10.12973/eu-jer.10.1.97>
- [11] L. Austen, M. Jones and A.-S. Wawera, "Exploring digital stories as research in higher education", Social Research Practice - SRA Journal, 7, 27-34, 2018. [Online]. Available <https://shura.shu.ac.uk/23345/13/Austen-ExploringDigitalStories%28AM%29.pdf> [Accessed Nov. 25, 2025].
- [12] M. Foelske, "Digital storytelling: the impact on student engagement, motivation and academic learning". Graduate Research Papers. 167. 2014. [Online]. Available pers. 167. <https://scholarworks.uni.edu/grp/167> [Accessed Nov. 18, 2025].
- [13] A. Leandro, J. Morais, and E. Silva, "Digital Storytelling in Higher Education: The Use of Podcasts in Building Institutional Identity and Engagement", *Innov High Educ*, 51, pp. 905-924, 2026. <https://doi.org/10.1007/s10755-025-09839-4>
- [14] Y. Tian, and N. Mohd Suki, "Evaluating Future Trends of Digital Storytelling in Higher Education: A Bibliometric Analysis", *International Journal of Interactive Mobile Technologies*, 17(17), pp. 121-133, 2023. <https://doi.org/10.3991/ijim.v17i17.39121>
- [15] P. A. Towndrow, "The multimodal meaning-making potential of self-representation and self-expression in digital storytelling", *Multimodality & Society*, vol. 3, no. 1, pp. 82-89, 2023. Available <https://journals.sagepub.com/doi/pdf/10.1177/26349795221140023> [Accessed January 21, 2025], <https://doi.org/10.1177/26349795221140023>
- [16] N. Smeda, E. Dakich, and N. Sharda, "The effectiveness of digital storytelling in the classrooms: a comprehensive study," *Smart Learning Environments*, 1: 6, 2014. [Online]. Available <https://link.springer.com/content/pdf/10.1186/s40561-014-0006-3.pdf> [Assessed Jan. 15, 2026]. <https://doi.org/10.1186/s40561-014-0006-3>

Students' Perceptions of Using AI Instruments in Developing Learning-to-Learn Skills: An Exploratory Qualitative Study

Oleksandr Malykhin
Department of Didactics
Institute of Pedagogy of NAES of
Ukraine
Kyiv, Ukraine
orcid.org/0000-0001-6042-6298

Nataliia Aristova
Department of International
Relations and Research Cooperation
Institute of Pedagogy of NAES of
Ukraine
Kyiv, Ukraine
orcid.org/0000-0002-0943-8039

Liudmyla Dybkova
Department of Informatics and
Systemology
Kyiv National Economic University
named after Vadym Hetman
Kyiv, Ukraine
orcid.org/0000-0002-3920-118X

Abstract—Considering the rapid evolution of digital technologies and the emergence of AI, within the Fourth Industrial Revolution university training should equip students with knowledge and skills to address the challenges of the labour market and, more importantly, successfully navigate their daily personal and professional lives. This implies teaching university students to use innovative digital technologies, including AI tools. Given the ongoing development of digital technologies, learning in the 21st century is a significant challenge. Although the use of AI tools in the university classroom raises many controversial issues, it is apparent that AI, as one of the newest digital technologies, is already an inseparable part of students' lives. The paper aims to understand students' perceptions of AI and its potential to develop their learning-to-learn skills. The researchers used a voluntary response sampling technique to select the research sample. To collect basic data on students' perceptions of using AI tools to develop their learning-to-learn skills, the researchers conducted an exploratory qualitative study. The findings indicate that the majority of students agree strongly that AI and AI tools open new opportunities for learning in general and for developing their learning-to-learn skills in particular.

Keywords—University students, learning-to-learn skills, AI tools, digital technologies.

I. INTRODUCTION

Digital technologies are rapidly evolving and constantly changing, as evidenced by the emergence of artificial intelligence, which is currently one of the key areas of their development. This statement also applies to the field of education, as educational systems (including higher education) worldwide are constantly evolving and seeking effective ways to improve instruction in response to today's challenges [1]. Considering education in general and higher education in particular as an open dynamic

system which tends to change with time, including the changes in its key components (i.e., teachers and students, instruction, teaching and learning approaches, technologies, methods and techniques, teaching and learning tools, etc.), it is worth mentioning that it always tries to take advantage of technologies advanced for their time. Within the Fourth Industrial revolution, equipping students with knowledge and skills to address the challenges of the labor market and, more importantly, successfully navigate their daily personal and professional lives implies teaching them to use innovative digital technologies, including AI tools [2; 3].

Regarding AI as a transformative force in higher education, Howard and Ulferts define it as “a pivotal tool to enhance student engagement, optimize administrative tasks, and democratize access to education” [4, p. 2].

Kwid, Sarty, and Yang believe that AI in education performs several functions, among which they distinguish personalization and/or differentiation of learning, provision of technical support during the evaluation process, and integration of adaptive learning platforms into the education process that adjust to students' needs [5].

Modern researchers are currently actively studying the impact of Artificial Intelligence (AI) and AI tools on the quality of education. Thus, for instance, Harry and Sayudin analyze the role and potential of AI in education [6]. The researchers conclude that one notable benefit of using AI tools in the classroom is the opportunity to personalize students' learning, thereby improving learning outcomes. Besides personalizing students' learning, the use of AI tools enables students to improve their efficiency and engagement [7].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.159>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Incorporating AI in the educational process can improve the performance of administrative tasks (including providing faster feedback to students), tailor more effective teaching and learning methods for students based on their individual educational preferences and interests, and, what seems to be also important, help teachers detect students' learning styles [8]. The use of AI tools leads to better teaching and learning, and, as a result, to better student learning outcomes, facilitated by the early identification of students' learning shortcomings and their correction. Moreover, the use of AI tools enables teachers to generate educational content that is responsive to students' needs, thereby helping students make more informed choices about their career paths.

While we acknowledge the idea expressed by Krstić, Aleksić, and Krstić that the use of AI tools reshapes the educational landscape, we argue that "traditional learning methods are becoming obsolete and various educational institutions are slowly rejecting them" [9, p. 227]. We believe that combining traditional teaching and learning methods with the use of innovative digital technologies, including AI, enables university teachers to provide students with a higher-quality education that can teach them to engage in lifelong learning, help them realize their full potential, and adapt more quickly to the rapidly changing requirements of the job market after graduating from higher educational institutions.

Although it is apparent that AI, as one of the newest digital technologies, is already an inseparable part of students' lives, its use in the university classroom still raises many controversial issues. Some researchers point out that AI education tools used in higher education provide teachers and students with excellent opportunities to make instruction more interactive and personalized [10; 11]. They point out that to help students succeed in their future careers, higher education institutions should implement advanced training and digital technologies in learning instruction. It is also evident that, as the most revolutionary technology, artificial intelligence enables higher education institutions to equip students with digital skills that help them stay at the forefront of technological progress [12]. At the same time, other researchers believe that AI can pose a serious threat to the quality of higher education, as their studies reveal that university teachers are concerned about data misuse, the facilitation of plagiarism, and privacy risks associated with AI tools [13; 14; 15].

Moreover, among other potential risks of AI that may adversely affect the quality of education, scientists also identify issues related to inequalities in access to AI systems, differences in teachers' and students' digital literacy, and academic integrity [14]. While focusing their attention on positive aspects of using AI in higher education, namely, improving the learning-teaching process, enhancing students' skills and competencies, better inclusion, and more efficient use of administrative resources, Pisica et al. also reveal some negative aspects of AI which include possible psychosocial effects, data security, ethical issues, unemployment threats, problems

related to the costs and efforts of implementing AI in higher education [15].

Thus, a literature review indicates that effective teaching and successful learning often depend on teachers' and students' knowledge, skills, and ability to use technological innovations in the classroom. It means that the skillful use of digital technology is one of the most important keys to effectively equipping students with the ability to learn lifelong and to acquire knowledge, skills, and expertise necessary for quickly adapting to new, non-standard situations in the workplace and to changing requirements in the labor market. The paper aims to understand students' perceptions of AI and its potential to develop their learning-to-learn skills. The decision to focus this research on how today's students perceive AI stems from the need to identify its positive potential for developing their learning-to-learn skills in the context of higher education's digital transformation. Paying close attention to the positive aspects and potential of AI in developing students' learning-to-learn skills may reveal the mechanisms of its effective use in the educational process and, at the same time, optimize the digital educational environment in higher education institutions.

II. MATERIALS AND METHODS

To collect basic data on students' perceptions of using AI tools to develop their learning-to-learn skills, the researchers conducted an exploratory qualitative study. To achieve the research aim, the researchers developed a questionnaire comprising open- and closed-ended questions. The questionnaire also includes several questions on demographic information, namely gender, age, and field of study. Given the current situation in Ukraine, which is marked by hostilities on its territory, the researchers considered it appropriate to use a mixed data collection approach. In this regard, the researchers developed two questionnaires in Ukrainian: paper-based and web-based. The researchers distributed questionnaires by hand where possible.

The researchers used a voluntary response sampling technique to select the research sample and the research sample consisted only of students who use AI for educational purposes. The sample comprised 119 students majoring in the following fields of study, namely, Marketing, Computer Science and English Philology, from National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine), Taras Shevchenko National University of Kyiv (Kyiv, Ukraine), Kyiv National University of Technologies and Design (Kyiv, Ukraine), Interregional Academy of Personnel Management (Kyiv, Ukraine), Kyiv National Economic University named after Vadym Hetman (Kyiv, Ukraine).

To find out students' perceptions of using AI tools to develop their learning-to-learn skills, both versions of the questionnaire included the following questions:

1. *How has your learning changed since you started using AI tools? Explain your answer.*
2. *What AI tools do you use for educational purposes?*

3. *In what ways do AI tools help you develop your learning-to-learn skills?*
4. *What exactly makes AI-based learning effective for developing your learning-to-learn skills?*
5. *Do AI tools provide you with any advantages in developing your learning-to-learn skills? Explain your point of view?*
6. *Can you assess your ability to use AI tools in developing your learning-to-learn skills?*

The mixed research design implies qualitative and quantitative data processing, including manual calculations.

The survey lasted four months, from September to December 2025.

III. RESULTS AND DISCUSSION

The results show that 64.71% of respondents are female (77 students) and 35.29% are male (42 students). 28.57% of respondents (34 students) are majoring in "Marketing", 26.89% (32 students) – in "Computer Science", and 44.54% (53 students) – in "English Philology".

The first question aims to determine how students' learning has changed since they started using AI tools. We infer from the results that the respondents' opinions on changes in their learning caused by AI tools were approximately identical. Table 1 presents general ideas from respondents' replies.

TABLE 1 RESPONDENTS' GENERALIZED IDEAS ON CHANGES CONNECTED WITH LEARNING CAUSED BY USING AI TOOLS

Respondents' Generalized Ideas	N	%
Help with translating information found in different sources	85	71.43
Assistance with explaining the educational material of any level of difficulty	104	87.39
A possibility to control one's own learning	67	56.30
Help in finding the information you need	110	92.44
Assistance in preparing presentations and visual materials	73	61.34
Help with organizing and structuring information	78	65.66
Assistance with tailoring educational material to individual needs	91	76.47
Equipping with new knowledge and skills	81	68.07

As we can see, respondents admit that their learning has changed due to the use of AI tools. The most noticeable change is the use of AI tools to find the information they need (92.44%). The only drawback was that the information they received often had to be verified. However, they saw some positives in this as well: by verifying the information, they gained a thorough understanding of the issue. Another positive idea was the possibility of getting help with explaining educational

material at any level of difficulty (87.39%). The students also noted that they can receive this assistance at any time. 73 respondents (61.34%) praised the AI assistance for tailoring educational material to their individual needs. They pointed out that they could explore the topics that interest them in greater detail. When searching for the information you need, you often have to analyze various sources written in different languages. Various tools that help translate this information are invaluable in this regard. You do not have to spend a lot of time translating; you can use AI tools and enjoy high-quality translations (71.43%). Many respondents (68.07%) believe that these tools help develop various skills useful in different fields, including digital skills.

The second question aims to determine what AI tools students use for educational purposes. Among the most popular answers, respondents mentioned DeepL Translate (81.51%), ChatGPT (100.00%), NotebookLM (42.86%), Canva (61.34%), Slides AI (44.54%), Gamma AI (38.66%), Microsoft Copilot (29.41%). The respondents consider them useful for preparing visual materials for their classes, finding the information they need, and translating sources from various languages.

Question 3 aimed to identify how AI tools help respondents develop their learning-to-learn skills. In response to this question, 82 respondents (69.91%) noted that being able to understand difficult material and get answers to their questions has a positive impact on their motivation and desire to learn. 65 respondents (54.62%) pointed out that the use of AI tools helps find and structure the information they need to complete homework assignments. However, we need to note that these respondents also recognized the fact that AI tools (especially ChatGPT) might present wishful thinking as fact. If you do not want to look into the matter and are not taking your studies seriously, this information could turn out to be false when verified. Such an attitude toward learning always leads to negative consequences. On the other hand, if you take your studies seriously, double-checking the information gives you the opportunity to gain a deeper understanding of the educational material. 49 respondents (41.18%) reported that the ability of AI tools to provide them with the opportunity to identify gaps in their knowledge and help them improve their knowledge according to their educational needs helps develop their learning-to-learn skills.

The researchers were also interested in what exactly makes AI-based learning effective for developing students' learning-to-learn skills. Table 2 demonstrates the results on this question.

TABLE 2 RESPONDENTS' REPLIES ON THE EFFECTIVENESS OF AI-BASED LEARNING IN DEVELOPING THEIR LEARNING-TO-LEARN SKILLS

Opinions	N	%
Identification of educational gaps and creation of tasks to address them	78	65.55
Better track the understanding of the educational material	53	44.54

Opinions	N	%
Explanation of any mistakes made and creation of exercises to help practice correcting them	46	38.66

78 respondents (65.55%) reported that using AI-based learning helps not only identify educational gaps (especially when preparing for seminars, practical classes, or exams), but also creates tasks to address them. Explaining their responses, they explained that by completing such tasks, students can receive immediate feedback and, if mistakes occur, focus more on correcting them. Moreover, AI-based learning allows users to adjust the difficulty level of the exercises to their current level of knowledge and vice versa. 53 respondents (44.54%) indicated that AI-based learning helps them better track their understanding of the material. For example, when using AI, students can ask it not only to create interactive exercises based on specific educational content, but also to check whether they completed them correctly. 46 respondents (38.66%) mention that they can also ask for explanations of any mistakes made and ask the AI to create exercises to help them practice correcting them. In its turn, involving students in creating various exercises using AI tools may positively influence their cognitive curiosity, leading them to seek more specific information and expand their personal educational experience.

The fifth question aims to determine whether using AI tools provides today's students with any advantages in developing their learning-to-learn skills. 65 respondents (54.62%) believe that applying AI inside and outside the classroom opens new opportunities to improve learning instruction, equipping students with new knowledge and skills. Moreover, using AI tools helps them stay up to date. 15 respondents (12.61%) find it difficult to answer this question, and 39 respondents (32.77%) maintain that modern digital technologies (including AI tools students use in their learning) have already proven their worth. They explain that to make the most of the advantages AI tools offer in developing learning-to-learn skills, students should thoroughly understand their features and know exactly how to apply them. Moreover, mastering and understanding all the subtleties takes some time.

Question 6 aims to assess students' ability to use AI tools to develop their learning-to-learn skills. Table 3 summarizes the obtained results.

TABLE 3 RESPONDENTS' SELF-ASSESSING THE ABILITY TO USE AI TOOLS IN DEVELOPING LEARNING-TO-LEARN SKILLS

Levels	N	%
High	18	15.13
Higher than moderate	25	21.01
Moderate	43	36.13
Low	33	27.73

The results indicate that most students assess their ability to use AI tools for developing their learning-to-learn skills as moderate (36.13%) or low (27.73%). Only a small proportion reported a high level of this ability (15.13%), while the majority demonstrated moderate or below-moderate self-assessment. This conclusion suggests that this ability is not sufficiently developed among a significant number of students and may require further support and targeted development. We may assume that such a perception of this ability is mostly related to the rapid development of digital technologies, including AI, and, as a consequence, to students' inability to even monitor the emergence of more refined AI tools. However, we also believe that access to, availability, and active use of various AI tools cannot guarantee a high level of this ability. Enhancing students' ability to use AI tools to develop their learning-to-learn skills requires a gradual, systemic, and purposeful implementation of AI in the educational process.

IV. CONCLUSIONS

Given that integrating AI into higher education is revolutionizing, and that the use of AI tools in teaching and learning opens up endless opportunities to improve the quality of higher education, the paper aimed to understand students' perceptions of AI and its potential to develop their learning-to-learn skills. The findings indicate that the majority of students agree strongly that AI and AI tools open new opportunities for learning in general and for developing their learning-to-learn skills in particular. Among the most noticeable changes associated with AI learning, respondents mention finding the necessary information, getting help explaining educational material at any level of difficulty, tailoring educational material to their individual needs, helping translate information from various resources, and developing skills useful in different fields, including digital skills.

The use of various AI tools for educational purposes helps today's students prepare visual materials for their classes, find the information they need, and translate sources from various languages. Moreover, it helps provide more personalized learning support, stimulate students' cognitive activity, has a positive impact on students' motivation and desire to learn.

The findings clearly demonstrate that students consider AI-based learning effective in improving their engagement and learning motivation, individualizing learning, addressing learning gaps and developing learning-to-learn skills.

The obtained results provide a basis for further research into the opinions of university teachers across different age groups regarding the impact of AI tools on the educational process in general and on the development of students' learning-to-learn skills in particular, which will enable them to be integrated more effectively into educational practice. Further research may also focus on revealing and comparing the positive and negative aspects of using AI to develop students' learning-to-learn skills, given the

controversy surrounding this didactic phenomenon in contemporary educational discourse.

V. STUDY LIMITATIONS

The key limitations of the study are the relatively small sample size, which may limit the generalizability of the findings, and its exclusive focus on the positive aspects of AI use in developing students' learning-to-learn skills. Given that the negative effects of implementing AI in higher education are not analyzed in this research, it may also narrow the comprehensiveness of the interpretation of the obtained findings.

REFERENCES

- [1] UNESCO, "Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development", Education Center [Online]. 2019. ED-2019/WS/8. Available: <https://repositorio.minedu.gob.pe/bitstream/handle/20.500.12799/6533/Artificial%20intelligence%20in%20education%20challenge%20and%20opportunities%20for%20sustainable%20development.pdf?sequence=1%26isAllowed=y> [Accessed: Dec. 18, 2025].
- [2] S. D. Bedir Erişti, and K. Freedman, "Integrating Digital Technologies and AI in Art Education: Pedagogical Competencies and the Evolution of Digital Visual Culture," Participatory Educational Research, vol. 11, pp. 57-79, Dec. 31, 2024. <https://doi.org/10.17275/per.24.94.11.6>
- [3] M. I. Qureshi, N. Khan, H. Raza, A. Imran, and F. Ismail, "Digital Technologies in Education 4.0. Does it Enhance the Effectiveness of Learning? A Systematic Literature Review. International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 04, pp. 31-47, 2021. <https://doi.org/10.3991/ijim.v15i04.20291>
- [4] T. L. Howard, and G. W. Ulferts, "Artificial Intelligence and the Redefinition of Higher Education," Research in Higher Education Journal, vol. 46, 2025. [Online]. Available <https://files.eric.ed.gov/fulltext/EJ1478931.pdf> [Accessed Nov. 21, 2025].
- [5] G. Kwid, N. Sarty, and D. Yang, "A Review of AI Tools: Definitions, Functions, and Applications for K-12 Education", ACRT, vol. 3, pp. 1-22, Nov. 2024. <https://doi.org/10.5772/acrt.20240048>.
- [6] A. Harry, S. Sayudin, "Role of AI in Education," INJURITY: Journal of Interdisciplinary Studies, vol. 2, no. 3, pp. 260-268, March 2023. <https://doi.org/10.58631/injury.v2i3.52>
- [7] O. Malykhin, N. Aristova, and L. Dybkova, "Using AI Tools for Personalising Learning in the English Language Classroom: Computer Science Undergraduate Students' Perceptions," ETR, vol. 3, pp. 213-217, June 8, 2025. <https://doi.org/10.17770/etr2025vol3.8536>
- [8] L. Chen, P. Chen, and Z. Lin, "Artificial Intelligence in Education: A Review", IEEE Access, vol. 8, pp. 75264-75278, April 17, 2020. <https://doi.org/10.1109/ACCESS.2020.2988510>
- [9] L. Krstić, V. Aleksić, and M. Krstić, Artificial Intelligence in Education: A Review: Technics and Informatics in Education – TIE 2022, pp. 223-228, September 16-18, 2022. [Online]. Available https://www.researchgate.net/publication/363100827_Artificial_Intelligence_in_Education_A_Review [Accessed Jan. 17, 2026]. <https://doi.org/10.46793-tie22-223k/>
- [10] V. Kuleto, M. Ilić, M. Dumangiu, M. Ranković, O. M. D. Martins, D. Păun, and L. Mihoreanu, "Exploring Opportunities and Challenges of Artificial Intelligence and Machine Learning in Higher Education Institutions," Sustainability, vol. 13(18), 10424, Sept. 18, 2021. <https://doi.org/10.3390/su131810424>
- [11] A. M. Vieriu, and G. Petrea, "The Impact of Artificial Intelligence (AI) on Students' Academic Development," Educ. Sci., vol. 15(3), 343, 2025. <https://doi.org/10.3390/educsci15030343>
- [12] A. Aler Tubella, M. Mora-Cantalops, and J. C. Nieves, "How to teach responsible AI in Higher Education: challenges and opportunities", Ethics Inf Technol, vol. 26, 3, 2024. <https://doi.org/10.1007/s10676-023-09733-7>
- [13] M. Pikhart, and L. H. Al-Obaydi, "Reporting the potential risk of using AI in higher Education: Subjective perspectives of educators", Computers in Human Behavior Reports, vol. 18, 100693, 2025. <https://doi.org/10.1016/j.chbr.2025.100693>.
- [14] M. Özer, "Potential Benefits and Risks of Artificial Intelligence in Education," Bartın University Journal of Faculty of Education, 13(2), 232-244, 2024. <https://doi.org/10.14686/buefad.1416087>
- [15] A. I. Pisica, T. Edu, R. M. Zaharia, & R. Zaharia, "Implementing Artificial Intelligence in Higher Education: Pros and Cons from the Perspectives of Academics," Societies, 13, 118. 2023. <https://doi.org/10.3390/soc13050118>

Human - AI Collaboration in Secure System Development: Decision Processes and Organizational Implications

Marina Marinova-Stoyanova

Department of Industrial Management
Technical University of Varna
Varna, Bulgaria
mpmstoyanova@tu-varna.bg

Boris Gramchev

Department of Industrial Management
Technical University of Varna
Varna, Bulgaria
gramchev@gmail.com

Abstract—Artificial intelligence is increasingly embedded in secure software development, yet its impact on security outcomes depends less on technical capability than on the socio-technical integration of its outputs. This paper examines human - AI collaboration, focusing on the critical interface between automated decision-support tools and team-level decision-making. Adopting an interdisciplinary perspective, the study analyzes how AI-generated insights inform threat modeling, risk assessment, and security architecture design. The paper proposes the Human-AI Decision Framework (HADF) as an analytical framework for organizing the interaction between AI outputs, human expertise, team deliberation, and organizational context. It identifies key organizational moderators - including trust, explainability, and coordination - that shape whether AI enhances security or introduces new vulnerabilities through misalignment risks. In doing so, the study bridges a gap between technical AI capability and the social processes through which security decisions are actually formed. By positioning AI as a supporting actor within a dynamic organizational system, the study provides a grounded foundation for future empirical research on AI-driven security governance. The framework also offers a structured basis for operationalizing human - AI collaboration in security-critical environments, enabling more consistent evaluation and refinement of decision practices.

Keywords—artificial intelligence (AI), decision-making processes, human - AI collaboration, organizational factors, secure system development

I. INTRODUCTION

Securing complex software systems has emerged as one of the most pressing challenges facing modern organizations. The proliferation of interconnected platforms, the layered nature of contemporary architectures, and the relentless pace at which cyber threats evolve have collectively placed organizations in a position of sustained vulnerability. What makes this particularly difficult to manage is that security is not

reducible to a technical problem alone - it is bound up with how teams read situations, weigh competing risks, and act under conditions of pressure and incomplete information [1]. Against this backdrop, the expanding role of artificial intelligence in software engineering and cybersecurity is changing what informs these decisions, even as the decisions themselves remain firmly in human hands [2].

Artificial intelligence has found its way into a wide range of tools that practitioners rely on during secure system development. It contributes to vulnerability detection, threat modeling, anomaly identification, and risk assessment - tasks that involve processing volumes of data and surfacing patterns that would otherwise escape human notice [3]. Code analysis tools, intrusion detection systems, and automated security monitoring platforms all reflect this integration in practice. Yet for all their capability, these tools do not make decisions. They produce outputs that someone must interpret, interrogate, and situate within a technical and organizational reality that no algorithm fully grasps [4]. This is where a meaningful tension arises. AI strengthens analytical capacity and compresses the time it takes to flag potential threats. But the weight of decision-making does not shift accordingly. Choices about security architecture, about which vulnerabilities warrant immediate attention, about how much risk is tolerable - these belong to teams that bring together developers, security specialists, and managers, each operating with their own constraints and framings [5]. AI-generated insights thus enter an environment that is already socially and organizationally complex, and their value depends less on computational accuracy than on how they are received and acted upon [6].

The motivation for this study lies in what that gap reveals. Research on AI in cybersecurity has largely focused on the performance of detection techniques, leaving largely unexamined how those systems actually interact with human decision-making in live development

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.133>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

contexts. There is a notable absence of conceptual frameworks that trace how AI outputs move through interpretation and deliberation to become collective decisions. This gap matters. When AI recommendations are misread, when automated outputs are accepted uncritically, or when team coordination is weak, the result can be not only a degradation of security practice but the introduction of new vulnerabilities [7] [8].

The present study approaches this problem through a conceptual and analytical lens, drawing on an integrative review of literature spanning artificial intelligence, software security, and team decision-making. Rather than testing a hypothesis against empirical data, the aim is to construct a coherent account of how human-AI collaboration operates within secure development settings. This approach is well suited to fields that remain fragmented and still taking shape, where the prior task is to organize insights from disparate domains into a framework that can support further inquiry [9]. The analysis centers on the nature of interaction between AI systems and human actors, and on the conditions that determine whether that interaction strengthens or undermines effective decision-making.

The central objective of the paper is to develop a conceptual framework that accounts for how AI-based decision-support tools are absorbed into team-level decision processes during secure system development - examining AI as a supporting actor rather than an autonomous one, understanding how teams make sense of and act on AI-generated insights, and identifying the organizational conditions that shape both, including trust, interpretability of outputs, and coordination structures within development teams.

The study offers a three-part contribution. It proposes a structured analytical framework that integrates AI systems, human expertise, team decision processes, and organizational context into a unified conceptual synthesis. It draws a connection between research on AI in cybersecurity and the established literature on team decision-making - a connection that has remained largely implicit. And it draws attention to risks inherent in human-AI collaboration, particularly the misalignment between automated recommendations and human judgment, a problem that has received insufficient attention in the literature. By treating secure system development as a genuinely collaborative endeavor between people and intelligent systems, the paper lays groundwork for both more rigorous research and more thoughtful practice.

II. ARTIFICIAL INTELLIGENCE IN SECURE SYSTEM DEVELOPMENT

AI has become a genuine part of how secure systems are built, particularly in areas that demand the analysis of large data volumes and the detection of patterns that manual review would struggle to catch. Its adoption reflects a broader move toward automation and data-driven support in software engineering. In security contexts, AI is primarily put to work in vulnerability

detection, threat modeling, and risk assessment across systems of growing complexity [3], [4].

Vulnerability detection represents possibly the most mature application of AI in this domain. Machine learning models woven into static and dynamic code analysis tools can scan software for weaknesses at a scale and speed that manual review simply cannot sustain. Intrusion detection systems take a similar approach, tracking behavioral patterns and surfacing anomalies that might otherwise go unnoticed until a breach has already occurred. Both applications prove especially valuable in environments where threats shift faster than any predetermined ruleset can keep up with [1].

Threat modeling and risk analysis represent a different but equally significant contribution. Drawing on historical data and documented attack patterns, AI systems can estimate the likelihood and potential impact of emerging threats, giving development teams a more principled basis for deciding where to focus their efforts. Rather than responding to incidents after the fact, teams can adopt a more anticipatory stance [3]. Continuous monitoring tools extend this further, supporting security as an ongoing discipline throughout the development lifecycle - a principle that sits at the heart of practices like DevSecOps [10].

That said, the limitations of these tools deserve equal attention. False positives and false negatives are a stubborn reality: systems that misclassify benign elements as threats, or overlook actual vulnerabilities, gradually undermine the confidence practitioners place in them. The problem deepens in complex systems where context is everything, and where AI models frequently lack the situational understanding needed to tell the difference.

Transparency compounds this. Deep learning models in particular tend to produce outputs without revealing their reasoning, which makes assessing reliability difficult. In environments where decisions carry real accountability, that opacity is not merely inconvenient - it actively discourages reliance [8].

Data quality presents a further constraint that no algorithmic refinement can fully resolve. Models trained on incomplete, biased, or outdated data will produce unreliable predictions, and the continuous emergence of novel attack types means that even well-trained systems struggle to generalize beyond what they already know.

What follows from all of this is a straightforward argument for sustained human oversight. AI is well suited to surfacing patterns and generating signals - but contextual awareness, sound judgment, and accountability are qualities it does not possess. Human experts remain responsible for interpreting what AI produces, evaluating its relevance, and deciding how to act. This is precisely what broader research on human-AI interaction has long maintained: the value of AI lies in extending human capability, not in replacing it [7], [11].

What this means in practice is that AI should be understood as a tool that informs judgment rather than one

that substitutes for it. The effectiveness of AI in secure development is therefore not primarily a question of technical performance - it is a question of how well AI outputs are integrated into human workflows and team processes. Outputs that are dismissed offer no value. Outputs that are accepted without critical reflection introduce risks of their own. Finding the right balance calls for reliable technology, but also for organizational practices that are thoughtfully designed around the genuine limits of automation.

From this perspective, integrating AI into secure system development is both an opportunity and a complication. It brings analytical power that can meaningfully improve security outcomes, while simultaneously introducing new dependencies and new forms of uncertainty. Understanding that tension clearly is what makes it possible to design processes that draw on AI's strengths without being quietly undermined by its weaknesses.

III. DECISION PROCESSES IN SECURE SOFTWARE DEVELOPMENT TEAMS

Decision-making in secure software development resists reduction to technical evaluation alone. It involves reading situations under uncertainty, balancing priorities that pull in different directions, and coordinating people whose expertise does not naturally converge. In security-critical environments, decisions must be made with incomplete information, under time pressure, and in the face of risks that resist precise quantification. This makes the process fundamentally cognitive and social rather than strictly analytical [5], [12].

At its core, the work revolves around identifying risks, assessing their likely impact, and determining what response is appropriate. These activities rarely occur in neat sequence. The moment a vulnerability is identified, questions about severity, urgency, and feasibility of mitigation tend to arise simultaneously. Teams find themselves constantly weighing whether a given risk demands immediate action, while also holding in mind the implications for performance, usability, and delivery timelines. Managing that balancing act is one of the defining features of secure development as a practice [4].

The people involved typically include developers, security specialists, architects, and project managers — each shaped by different responsibilities and different definitions of what counts as a problem. Developers think in terms of implementation and efficiency; security specialists in terms of exposure; architects in terms of system-wide coherence; managers in terms of resources and deadlines. These orientations do not naturally align, and the tension they produce cannot be engineered away - it has to be worked through in discussion [13].

The introduction of AI-based tools adds another dimension to this already layered process. These tools surface alerts, generate risk scores, and offer recommendations that can shift how problems are initially perceived. What they do not do is eliminate uncertainty. The question becomes how much weight to assign to what

the AI is reporting, and how to fold those outputs into existing workflows. Because AI systems operate without full awareness of operational context, their outputs demand careful judgment rather than straightforward acceptance. A flagged vulnerability may be technically accurate but practically irrelevant - or equally, the reverse.

One persistent challenge is that the same AI output can mean different things to different people. A security engineer and a developer reading the same risk assessment may reach very different conclusions, each filtering the information through their own expertise. These differences reflect the genuinely multi-dimensional nature of secure development, but they can harden into disagreement or produce delays when no shared interpretation emerges.

Cognitive load presents a related difficulty. AI tools produce substantial volumes of output - alerts, indicators, ranked risk lists - all competing for attention within teams that are already stretched. As that effort depletes, people fall back on heuristics rather than careful analysis, which is precisely when important signals are most likely to be missed or misread [12]. The risk is not that teams ignore AI outputs entirely, but that they engage with them selectively and in ways that introduce their own blind spots.

Coordination, meanwhile, is not a background condition but an active requirement. Effective decision-making depends on team members being able to share what they know, build enough common ground to discuss it meaningfully, and agree on a course of action. Where that alignment is absent, even accurate insights can fail to translate into coherent decisions [11].

Decision-support systems are generally expected to improve both the quality and speed of team choices. In practice, their effect depends almost entirely on how they are integrated into the work. Outputs that are not trusted tend to be set aside. Outputs that are trusted too readily tend to be accepted without adequate scrutiny. The real challenge is sustaining the kind of calibrated judgment that knows when each response is appropriate [4].

What emerges is a view of decision-making in secure software development as simultaneously collective and interpretive. It is collective because no single actor holds enough perspective or authority to carry it alone. It is interpretive because information - including AI-generated information - does not arrive pre-loaded with meaning. Meaning is constructed through discussion, through validation against other sources, and through the particular context in which a team operates. Seen in this light, AI does not replace human decision-making. It becomes one input among many in a process that remains, at its core, social, negotiated, and deeply context-dependent.

IV. THE HUMAN-AI DECISION FRAMEWORK (HADF) FOR SECURE SYSTEM DEVELOPMENT

The integration of artificial intelligence into secure system development does not displace human decision-

making - it reshapes the conditions under which decisions are formed, negotiated, and carried through. The framework proposed here conceptualizes secure development as a multi-layered interaction between AI-based decision-support systems, human expertise, team-level decision processes, and the broader organizational context in which all of these are embedded. Rather than casting AI as an autonomous actor, the framework positions it as an analytical component within a socio-technical system where meaning, judgment, and responsibility remain distributed among human participants. This view is consistent with research arguing that effective human - AI interaction depends not only on what a system can do, but on how its outputs are interpreted and put to use in practice [8] [7].

At its core, the framework identifies four interdependent components. The first is the AI decision-support system itself, which provides analytical capabilities including threat detection, vulnerability identification, and risk assessment. Operating on large datasets and probabilistic models, these systems produce outputs that flag potential security issues or rank risks by priority. Yet as the automation literature has long established, such outputs are inevitably incomplete representations of a more complex reality and cannot be acted upon without human interpretation [11].

The second component is human expertise. Developers and security specialists bring contextual knowledge, accumulated experience, and domain understanding that allow them to assess the relevance of AI-generated insights and determine whether and how to act on them. This interpretive function becomes especially critical when AI outputs are uncertain, ambiguous, or appear to contradict one another.

The third component is the team-level decision process. Secure system development is not a matter of individual judgment - it involves collective evaluation, negotiation, and prioritization of security concerns. Teams must simultaneously balance competing demands around performance, usability, cost, and risk, while coordinating across areas of expertise that do not always share the same vocabulary or the same priorities. Research on software development has consistently shown that these processes hinge on communication patterns, shared understanding, and coordination mechanisms [5], [6]. AI-generated insights enter this collective space and must be translated into shared meaning before they can meaningfully shape decisions.

The fourth component is system design and implementation. This is the point at which interpreted insights and team decisions are translated into concrete security measures, risk mitigation choices, and development actions. In other words, the framework does not end with analysis or discussion; it culminates in design and implementation outcomes that shape the secure system itself [4].

These four components are embedded within a broader organizational context, represented in Figure 1 as

the outer structure surrounding the core process, rather than as a separate component. This context includes policies and governance, culture and norms, and processes of learning and adaptation that shape how AI outputs are interpreted, how decisions are made, and how feedback from implementation re-enters the system over time.

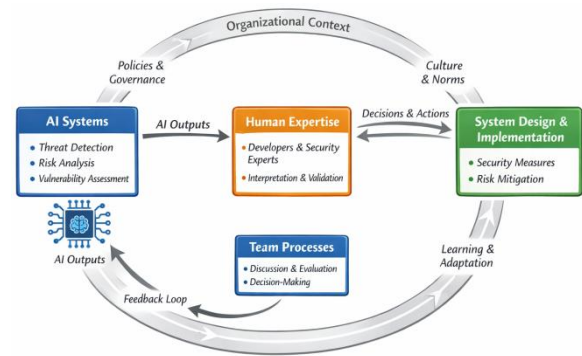


Fig. 1. The Human-AI Decision Framework (HADF) as a Conceptual Map of Secure System Development

Figure 1 should be read as a conceptual map of the human-AI decision environment rather than as a technical system architecture or a strictly sequential workflow. It synthesizes the main elements involved in secure system development — AI systems, human expertise, team decision processes, and organizational context — and shows how they interact within a broader socio-technical setting. The interaction mechanisms discussed in the following paragraphs, including interpretation, validation, challenge, and feedback, operate across these elements and explain how AI-generated outputs become part of team-level security decisions.

The relationship between these components is not sequential but iterative and continuously evolving. AI systems generate outputs from available data; these outputs are interpreted by individuals and brought into team discussions, where they are evaluated alongside other information and organizational constraints. The resulting decisions, implemented in system design and development, produce outcomes that generate new data and re-enter the system.

Central to the framework is a set of interaction mechanisms that mediate between AI outputs and human decision-making. The first is interpretation. AI systems produce signals - alerts, risk scores, recommendations - but signals do not carry inherent meaning. Meaning is constructed by the people who receive them, drawing on their understanding of the system, the development context, and what currently matters most. This process connects closely to the notion of situation awareness, in which effective decision-makers must grasp not only what is happening but why it is significant and what it demands of them [13].

The second mechanism is validation. AI-generated insights are rarely taken at face value. Practitioners typically cross-reference them against manual analysis,

prior experience, or parallel tools before acting. Validation functions as a check against overreliance on automated systems, reducing the risk of acting on outputs that are incorrect or misleading. At the same time, excessive skepticism can blunt the benefits of AI support and slow down decision cycles, which points to the importance of calibration rather than blanket acceptance or dismissal [14].

The third mechanism is challenge. Within teams, the same AI output may be read differently by different people, and this can generate disagreement. That disagreement is not inherently problematic. When handled well, constructive challenge improves decision quality by surfacing hidden assumptions, revealing blind spots, and prompting more rigorous analysis. When poorly managed, it introduces friction and delays that can undermine the team's capacity to act. How much challenge helps rather than hinders depends heavily on team dynamics and the quality of communication within the group [15].

The fourth mechanism involves feedback loops between human actors and AI systems. The decisions teams make shape how systems are configured, what data gets collected, and how models evolve. Those changes, in turn, alter future AI outputs. This recursive relationship means that human-AI collaboration is not a fixed arrangement but one that develops and shifts over time. Iteration, in this sense, is not incidental to the framework - it is one of its defining features, reflecting the adaptive nature of secure system development as a practice [16].

AI systems generate analytical outputs that identify potential risks or vulnerabilities. Individual experts first encounter and assess these outputs, forming judgments about their relevance and reliability. Those judgments are then brought into team-level discussions, where they are weighed against competing priorities and organizational constraints. From that collective process, decisions emerge regarding design choices, implementation strategies, or mitigation approaches. This sequence - from AI output, through human interpretation, into team deliberation, and toward implementation - captures how data becomes action, and makes explicit that decision-making authority at no point passes out of human hands.

Beyond the core processes, the framework draws attention to several risks that arise when human judgment and AI outputs fall out of alignment. One is overreliance - the tendency to accept AI outputs without adequate scrutiny, often when systems carry a reputation for high accuracy or when time pressure leaves little room for validation. Research on automation has demonstrated that this kind of overtrust can produce serious errors, particularly in high-stakes settings [11]. The inverse risk is underutilization: AI outputs that are ignored or dismissed, typically because trust is absent or because users do not have a clear sense of how the system works. Here the potential value of AI goes unrealized. These risks manifest in practice as recognizable patterns, including overreliance, underutilization, divergent interpretation, decision delay, and accountability ambiguity. Rather than representing these risks as a causal

sequence, Table 1 summarizes them as distinct but potentially co-occurring forms of human-AI misalignment in secure system development.

TABLE 1. HUMAN-AI MISALIGNMENT RISKS IN SECURE SYSTEM DEVELOPMENT

Misalignment risk	Description	Possible consequence
Overreliance on AI	AI outputs are accepted without sufficient human scrutiny	Incorrect recommendations may shape security decisions
Underutilization of AI	AI outputs are ignored or dismissed due to low trust	Useful signals may remain unused
Divergent interpretation	Different experts assign different meaning to the same AI output	Inconsistent prioritization and conflict
Decision delay	Teams struggle to reconcile AI outputs with existing knowledge or procedures	Slower response to security threats
Accountability ambiguity	Responsibility for AI-influenced decisions is unclear	Weak governance and reduced decision ownership

These risks should not be understood as outcomes of the technology alone. They emerge from the interaction between AI systems, human users, team processes, and organizational structures. For this reason, Table 1 presents them as distinct but potentially co-occurring forms of misalignment rather than as a causal sequence.

Taken together, these components, mechanisms, and misalignment risks constitute a framework for understanding how AI becomes part of secure system development in practice. The central argument is that the effectiveness of AI is not a function of technical performance in isolation, but of how well it is woven into human and organizational processes. This shifts the question from what AI is capable of to how it is actually used - and in doing so, offers a more grounded basis for both research and real-world implementation. At the same time, it suggests that the role of AI in secure development may vary significantly across organizational contexts, an issue that warrants further empirical attention.

V. ORGANIZATIONAL FACTORS INFLUENCING HUMAN-AI COLLABORATION

The effectiveness of artificial intelligence in secure system development is not determined by technical capability alone. It depends, in equal measure, on the organizational environment into which these systems are introduced. AI tools do not operate in a vacuum - their outputs land within teams shaped by norms, expectations, and institutional pressures that vary considerably from one setting to another. The same technology, deployed under different conditions, can produce very different results [17].

Trust is perhaps the most consequential of these conditions. It governs whether team members engage seriously with AI-generated insights, treat them with skepticism, or set them aside entirely. Trust is not a fixed state - it sits on a spectrum and shifts as people accumulate experience with a system. When it runs too low, genuinely useful outputs get dismissed. When it runs too high, outputs get accepted without the scrutiny they may warrant, and the risk of consequential error rises accordingly [14]. In secure development, where the stakes of a wrong decision can be significant, calibrating trust appropriately is not optional. It requires both reliable system performance and honest communication about what AI tools can and cannot do.

Transparency and explainability bear directly on this. Many AI systems - particularly those built on complex machine learning models - produce results without revealing how those results were reached. For practitioners, this is a practical obstacle. Defending a decision in a professional or institutional context is difficult when the reasoning behind it remains opaque. Explainability does not need to be technically exhaustive; it needs to be meaningful to the people actually using the system. When it is, interpretation improves and decision-making becomes more grounded. When it is absent, both trust and usability tend to suffer [8].

Team coordination shapes outcomes just as significantly as the tech itself. Secure system development is inherently a collective endeavor, and introducing AI tools doesn't change that reality-it simply adds a new stream of information that people must share, discuss, and make sense of together. Effective coordination requires clear communication practices, a shared understanding across different areas of expertise, and well-defined roles. Teams need to work out exactly how AI outputs enter their conversations, who carries the responsibility for validating them, and how disagreements about their meaning get resolved. Without that structure, insights tend to remain fragmented or get applied inconsistently [13].

Governance matters for similar reasons. Organizations need to define how AI is used, who is accountable for decisions it influences, and what standards apply. But governance, in this sense, extends well beyond formal policy documents. It lives in the everyday practices through which decisions get made, risks get assessed, and responsibility gets distributed. In secure development, this might mean setting thresholds for action based on AI outputs, building review processes into existing workflows, or ensuring that AI tools are integrated coherently with broader security frameworks [4]. Good governance ensures that AI reinforces established practice rather than cutting across it.

Organizational learning deserves more attention than it typically receives in this conversation. The relationship between human teams and AI systems is not static - it evolves. People learn to read outputs more accurately, recognize patterns in system behavior, and refine how they respond. AI systems, in turn, are updated as new data becomes available and as user feedback accumulates. This

creates a reciprocal process of adaptation, and organizations that invest in supporting it - through training, reflection, and a willingness to revisit their practices - tend to derive considerably more from AI integration than those that treat deployment as an endpoint rather than a beginning [18].

Cultural factors, less visible but no less real, also play a role. Digitalisation processes are placing new demands on human resources [19]. Attitudes toward technology, comfort with uncertainty, and the degree to which human judgment is valued over automated outputs all color how AI is perceived and used. Some environments are instinctively resistant to automation; others lean on it too heavily. Neither disposition serves well. What effective human-AI collaboration actually requires is a more measured orientation — one that treats AI as a resource worth engaging with critically, rather than something to be either embraced wholesale or held at arm's length [4]. These factors can be understood as mutually reinforcing conditions shaping the calibration of human-AI interaction. To clarify their practical role, Table 2 summarizes the main organizational factors shaping human-AI collaboration in secure system development.

TABLE 2. ORGANIZATIONAL FACTORS SHAPING HUMAN-AI COLLABORATION IN SECURE SYSTEM DEVELOPMENT

Organizational factor	Role in human-AI collaboration	Practical implication
Trust calibration	Determines whether AI outputs are accepted, questioned, or ignored	Teams need neither blind trust nor automatic rejection
Explainability	Supports interpretation and justification of AI-generated recommendations	Outputs should be understandable to practitioners
Team coordination	Enables shared interpretation across developers, security experts, and managers	Roles and validation responsibilities should be clear
Governance	Defines accountability and acceptable use of AI-supported decisions	AI use should be embedded in formal and informal decision rules
Organizational learning	Allows teams to refine how AI outputs are used over time	Feedback and training should accompany AI deployment
Culture and norms	Shape attitudes toward automation, judgment, and uncertainty	AI adoption depends on existing organizational assumptions

Table 2 summarizes the key organizational factors that shape how human - AI collaboration unfolds in secure system development. What all of this points toward is that integrating AI into secure system development is not simply a matter of acquiring new tools. It demands adjustments in how teams operate, how decisions get made, and how accountability is understood. Trust, transparency, coordination, governance, and learning do not function independently - they reinforce one another, and a weakness in any one of them can compromise the whole. Strong technical performance means little if trust is absent or coordination is poor. Organizational context, in

other words, is not background to the story of human–AI collaboration - it is the condition on which that collaboration either succeeds or falls short.

VI. DISCUSSION

The integration of artificial intelligence into secure system development changes how decisions are informed, but it does not change who is responsible for making them. This distinction is easy to overlook, especially when AI systems perform well. Yet, the findings suggest that their value depends less on accuracy alone and more on how teams engage with them in practice.

From a practical perspective, the framework points to a simple but often neglected idea: AI works best when it becomes part of the conversation, not a replacement for it. Teams need to actively interpret, question, and sometimes challenge AI outputs. This takes time. It also requires discipline. Without such engagement, even high-quality insights may remain unused or misunderstood. At the same time, too much skepticism can slow down decisions and reduce the benefits of automation. The challenge is not to choose between trust and doubt, but to manage both at the same time.

Another implication concerns how teams organize their work. AI introduces new types of information, but it does not automatically create shared understanding. That still has to be built. Teams that openly discuss AI outputs, clarify assumptions, and align their interpretations tend to make more consistent decisions. Those that do not often struggle with fragmentation. The difference is not in the technology, but in how it is used.

From a theoretical point of view, the study reinforces the idea that secure system development is not purely technical. It is a socio-technical process where tools, people, and structures interact continuously. AI fits into this process as an additional layer, not as a dominant one. This perspective challenges more deterministic views of automation and supports a more balanced understanding of human - AI collaboration. It also suggests that research on cybersecurity and software engineering needs to pay closer attention to team dynamics and organizational context.

There are, however, clear limitations. The framework is conceptual and does not rely on empirical validation within a specific organizational setting. It simplifies complex interactions in order to make them understandable, which means that some nuances are inevitably lost. In practice, different organizations may experience these dynamics in different ways, depending on their structure, culture, and level of technological maturity.

Even with these limitations, the discussion highlights a consistent point. AI does not remove uncertainty from secure system development. It redistributes it. Decisions still depend on interpretation, coordination, and judgment. The difference is that these processes now take place in an environment where part of the information is generated by

intelligent systems. Understanding this shift is essential for both researchers and practitioners.

VII. CONCLUSION

This study examined the role of artificial intelligence in secure system development through the lens of human–AI collaboration. Rather than treating AI as an autonomous decision-maker, the paper positioned it as a decision-support component embedded within team-based and organizational processes. The proposed framework highlights that security decisions emerge from the interaction between AI-generated insights, human expertise, and collective team dynamics, all shaped by the surrounding organizational context.

The findings suggest that the effectiveness of AI in secure development depends less on its technical performance alone and more on how it is interpreted, validated, and integrated into decision processes. Trust, explainability, coordination, and governance play a central role in determining whether AI contributes to better outcomes or introduces additional risks. In this sense, secure system development remains fundamentally a human-centered activity, even in highly automated environments.

The framework should be understood as a conceptual synthesis rather than an empirically validated model. Its purpose is to clarify the interaction between AI outputs, human expertise, team-level decision-making, and organizational context, and to provide a basis for future empirical research.

The study contributes by offering a structured analytical framework that organizes key components of human–AI collaboration in secure system development. At the same time, it opens several directions for future research, particularly the need for empirical validation of the framework and deeper exploration of how different organizational settings influence human - AI interaction.

REFERENCES

- [1] Casola, V., De Benedictis, A., Mazzocca, C., & Orbinato, V. (2024). Secure software development and testing: A model-based methodology. *Computers & Security*, 137, 103639. <https://doi.org/10.1016/j.cose.2023.103639>
- [2] NIST. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). National Institute of Standards and Technology.
- [3] Sarker, I.H., Furhad, M.H. and Nowrozy, R. (2021) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, 2, Article No. 173. <https://doi.org/10.1007/s42979-021-00557-0>
- [4] Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556(7701), 296–298. <https://doi.org/10.1038/d41586-018-04602-6>
- [5] Hamza, M., Younas, M., Hummel, M., & Sajjad, M. (2024). Human–AI collaboration in software engineering: A systematic mapping study. In *Proceedings of the 17th International Conference on Cooperative and Human Aspects of Software Engineering*. Association for Computing Machinery. <https://doi.org/10.1145/3643690.3648236>
- [6] Alhumam, A., & Ahmed, S. (2024). Software requirement engineering over the federated environment in distributed software development process. *Journal of King Saud University* –

- Computer and Information Sciences*, 36(9), 102201. <https://doi.org/10.1016/j.jksuci.2024.102201>
- [7] Amershi, S., Weld, D., Vorvoreanu, M., Fournery, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P. N., Inkpen, K., Teevan, J., Kikin-Gil, R., & Horvitz, E. (2019). Guidelines for human-AI interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 3, 13 pages. <https://doi.org/10.1145/3290605.3300233>
- [8] Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human-Computer Interaction*, 36(6), 495–504. <https://doi.org/10.1080/10447318.2020.1741118>
- [9] Snyder, H. (2024). Designing the literature review for a strong contribution. *Journal of Decision Systems*, 33(4), 551–558. <https://doi.org/10.1080/12460125.2023.2197704>
- [10] Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, 34(2), 101885. <https://doi.org/10.1016/j.jsis.2024.101885>
- [11] Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 30(3), 286–297. <https://doi.org/10.1109/3468.844354>
- [12] Klein, G. (2008). Naturalistic decision making. *Human Factors*, 50(3), 456–460. <https://doi.org/10.1518/001872008X288385>
- [13] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64. <https://doi.org/10.1518/001872095779049543>
- [14] Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 46, 50–80. https://doi.org/10.1518/hfes.46.1.50_30392
- [15] Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2), 627–660. <https://doi.org/10.5465/annals.2018.0057>
- [16] Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577–586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- [17] Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1), 366–410. <https://doi.org/10.5465/annals.2018.0174>
- [18] Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science*, 48(1), 137–141. <https://doi.org/10.1007/s11747-019-00710-5>
- [19] Narleva K., Narlev Y., Gancheva Y., (2023). Maritime Education and New Skills in the Digitisation Process, *HR and Technologies*, Creative Space Association, 2, 57-72.

AI-Enhanced Detection of ARP Spoofing-Based Man-in-the-Middle Attacks in Local Area Networks

Penka Markova

Computer Science and Engineering
Technical University of Varna
Varna, Bulgaria
penkamarkova5@gmail.com

Georgi Markov

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
g.markov@naval-acad.bg

Abstract—Man-in-the-Middle (MitM) attacks remain a significant threat to local area networks, particularly when implemented through Address Resolution Protocol (ARP) spoofing. Although infrastructure-level protection mechanisms such as Dynamic ARP Inspection (DAI) are effective against conventional ARP poisoning attempts, their detection capability is limited in low-rate and insider-like scenarios, where malicious behavior may appear formally valid while remaining anomalous in context. This paper proposes a hybrid LAN protection architecture that combines DAI with an AI-based behavioral detection module to improve the identification of stealthy and context-dependent MitM activity. The proposed approach analyzes ARP, DHCP, and switch-port events using interpretable traffic features and a two-stage detection logic that integrates anomaly filtering and supervised classification. The system was evaluated in a controlled laboratory environment under three attack scenarios: classic high-rate ARP spoofing, low-rate stealth spoofing, and insider spoofing. The experimental results show that DAI alone performs very well in classic spoofing conditions, but its effectiveness decreases substantially in low-rate and insider scenarios. In contrast, the proposed DAI+AI architecture achieves the best overall balance between recall, precision, F1-score, detection latency, and false positive rate. The findings indicate that AI can effectively complement traditional infrastructure-level network defenses by providing behavioral awareness and improved sensitivity to attack patterns that are difficult to detect through rule-based inspection alone.

Keywords— anomaly detection, ARP spoofing, artificial intelligence, behavioral analysis, Dynamic ARP Inspection, intrusion detection system, LAN security, Man-in-the-Middle attack.

I. INTRODUCTION

Modern enterprise networks are characterized by extensive interconnectivity, rapid expansion of communication services, and increasing integration of cloud platforms, mobile devices, and Internet of Things

(IoT) components. While this transformation improves flexibility and functionality, it also enlarges the attack surface and introduces new vulnerabilities across both local and distributed environments. In this context, securing communication channels at the local area network (LAN) level remains a critical element of overall cyber defense [1], [2].

Among the major threats to Ethernet/IP infrastructures are Man-in-the-Middle (MitM) attacks, in which an adversary positions itself between two communicating hosts in order to intercept, modify, or redirect traffic. In IPv4 LANs, one of the most common practical realizations of MitM is ARP spoofing (also referred to as ARP poisoning), where forged ARP messages are used to alter IP-to-MAC mappings in the ARP cache of network devices. As a result, traffic is redirected through the attacker-controlled host, enabling packet inspection, credential theft, session compromise, and further lateral exploitation [3], [4], [5].

The severity of ARP spoofing stems from the fact that the ARP protocol does not provide built-in sender authentication. Consequently, forged ARP replies and gratuitous ARP messages can update dynamic ARP entries on target hosts without any cryptographic verification. Prior studies have shown that ARP-based MitM attacks remain operationally relevant even in relatively simple LANs, particularly when combined with unencrypted services or poorly monitored internal segments [4], [6].

Traditional defenses against MitM attacks include cryptographic protection, static filtering rules, ARP inspection mechanisms, and signature-based intrusion detection and prevention systems. For ARP-specific attacks, Dynamic ARP Inspection (DAI) is one of the most widely deployed infrastructure-level countermeasures. DAI validates ARP messages against DHCP snooping bindings and/or statically configured IP-to-MAC associations, making it effective against obvious ARP

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.52>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

poisoning attempts. However, the literature indicates that rule-based defenses become less effective when malicious activity appears formally valid yet deviates from normal behavior in statistical, temporal, or contextual terms. Similar limitations are observed in signature-based IDS/IPS systems, which remain effective for known attack patterns but show limited adaptability to stealthy, evolving, or low-rate threats [6], [7], [8].

These limitations have motivated growing interest in artificial intelligence (AI) and machine learning (ML) for network security applications. Unlike strictly rule-based or signature-driven approaches, AI/ML models can identify anomalies by analyzing behavioral, statistical, and temporal dependencies in network traffic. Such methods are particularly suitable for attacks that manifest not through a single highly distinctive packet, but through weak yet correlated deviations over time. Existing research has demonstrated the applicability of both conventional ML algorithms, such as Decision Trees, Random Forests, and Support Vector Machines, and deep learning models, including recurrent neural networks (RNNs), Long Short-Term Memory (LSTM) networks, and hybrid architectures, for intrusion detection and anomaly analysis [8], [9], [10], [11].

Recent studies further indicate that specialized AI-based approaches can improve the detection of ARP-related attacks. For example, explainable deep learning has been applied to ARP spoofing detection in IoT settings, highlighting not only accuracy gains but also the importance of interpretability for network administrators and security operation teams [12]. At the same time, the literature still reports persistent challenges, including limited availability of realistic labeled datasets, restricted model explainability, and vulnerability to adversarial manipulation. These issues suggest that black-box AI models, although often effective, may not be sufficient on their own for practical deployment in operational environments [13], [14], [15].

Against this background, a clear research gap emerges between traditional infrastructure-level defenses and adaptive behavioral analysis. While the combination of AI techniques with rule-based security mechanisms is not entirely new, most existing approaches either focus on general-purpose intrusion detection or treat ARP spoofing as one of many attack classes within broader anomaly detection frameworks. In contrast, this paper focuses specifically on ARP spoofing-based MitM attacks in LAN environments and evaluates how infrastructure-level ARP validation can be enhanced by AI-driven behavioral analysis of ARP, DHCP, and switch-port related events.

Rather than replacing established mechanisms such as DAI, the proposed approach augments them with an intelligent analytical layer capable of detecting low-intensity, context-dependent, and insider-like anomalies that may not be sufficiently visible to static validation rules alone. The main contribution of the paper is therefore not the isolated use of AI, but the experimental evaluation of a hybrid DAI+AI architecture under controlled ARP-based MitM attack conditions. The study compares DAI-only, AI-only, and DAI+AI configurations in order to assess

whether the hybrid approach improves detection sensitivity while preserving the operational advantages of conventional network defenses.

II. MATERIALS AND METHODS

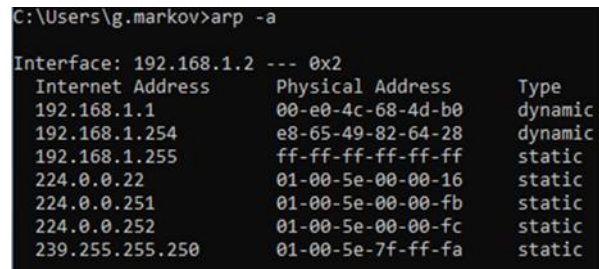
A. Experimental Objective

The objective of this study is to evaluate the effectiveness of a hybrid defense approach against MitM attacks in local area networks, based on the combination of DAI and an AI-based behavioral detection module. The proposed architecture is designed to determine whether the integration of infrastructure-level ARP validation and intelligent anomaly detection can improve sensitivity to low-rate and insider-like ARP-based attacks that may remain undetected by purely rule-based mechanisms.

B. Experimental Setup and Attack Scenarios

The experiments were conducted in a controlled laboratory LAN environment designed to reproduce realistic ARP-based MitM attack conditions. The test topology included a client host (192.168.1.2), router R1 (192.168.1.1), a gateway device (192.168.1.254), an attacker machine running Ettercap, a Layer-2 Cisco switch with DAI enabled, and a separate NIDS/AI host connected via a SPAN port. The AI module received mirrored traffic for feature extraction and event analysis.

Before attack execution, the initial ARP state of the participating devices was verified in order to confirm valid and stable IP-to-MAC associations. This baseline state is illustrated in Fig. 1. A period of normal traffic was then collected to establish a reference profile for benign ARP behavior. The attacker-side configuration used for ARP spoofing is shown in Fig. 2.



Internet Address	Physical Address	Type
192.168.1.1	00-e0-4c-68-4d-b0	dynamic
192.168.1.254	e8-65-49-82-64-28	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Fig. 1. Initial ARP state before attack execution.

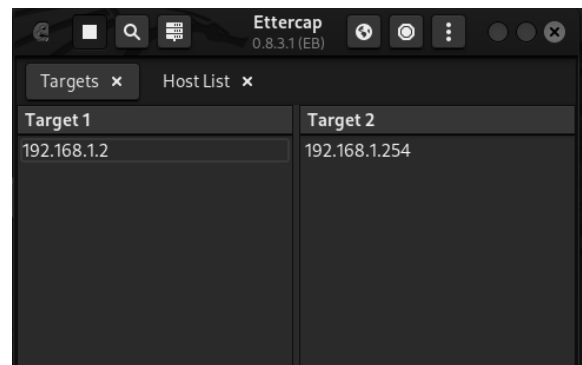


Fig. 2. Ettercap configuration for ARP spoofing execution.

Three attack scenarios were defined for evaluation:

- Scenario A – classic high-rate ARP spoofing: frequent forged ARP replies and gratuitous ARP messages were injected in order to rapidly poison the ARP cache of the victim and the gateway;
- Scenario B – low-rate stealth spoofing: forged ARP messages were sent at lower frequency and with longer intervals to reduce the likelihood of threshold-based detection.
- Scenario C – insider spoofing: the attack was performed from a compromised legitimate host, simulating an internal adversary with apparently valid network presence.

The attacks were executed using Ettercap configured for ARP spoofing between the victim host and the gateway. The resulting change in ARP associations after successful poisoning is illustrated in Fig. 3.

```
C:\Users\g.markov>arp -a
```

Interface: 192.168.1.2 --- 0x2		
Internet Address	Physical Address	Type
192.168.1.1	00-e0-4c-68-4d-b0	dynamic
192.168.1.3	30-9c-23-d9-81-61	dynamic
192.168.1.254	e8-65-49-82-64-28	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

```
C:\Users\g.markov>arp -a
```

Interface: 192.168.1.2 --- 0x2		
Internet Address	Physical Address	Type
192.168.1.1	00-e0-4c-68-4d-b0	dynamic
192.168.1.3	30-9c-23-d9-81-61	dynamic
192.168.1.254	e8-65-49-82-64-28	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Fig. 3. Modified ARP entries after successful ARP spoofing.

C. Data Collection and Feature Extraction

For each experiment, packet captures (pcap files), DAI logs, DHCP bindings, and MAC-to-port history records were collected. In addition to real-time monitoring through the SPAN port, an offline replay mode based on previously recorded pcap files was used in order to safely and repeatedly test the low-rate and insider scenarios.

A set of simple and interpretable features was extracted from the collected pcaps and logs for subsequent detection. These features included the number of ARP packets, the number of gratuitous ARP messages, the number of IP-to-MAC mapping changes, MAC address entropy, correlation with DHCP binding information, and changes in switch port association. The use of explainable features was intentionally preferred in order to support practical interpretability, easier forensic analysis, and smoother integration with network administration workflows.

Traffic analysis was performed using two time windows: a short window of 60 s for rapid detection of abrupt anomalies and a longer window of 300 s for detecting weaker, temporally distributed deviations typical of low-rate and insider attacks.

The extracted feature vectors were normalized before being provided to the AI module, so that features with different numerical ranges, such as packet counts and entropy values, would not disproportionately influence the classification process.

D. Hybrid DAI+AI Detection Model

The proposed system follows a two-stage detection logic. In the first stage, an unsupervised anomaly detection module is used to identify deviations from the baseline profile of normal LAN behavior. In the experimental implementation, this stage is based on the analysis of ARP-related and flow-level features extracted over 60 s and 300 s observation windows. The purpose of this stage is to detect unusual changes in ARP activity, IP-to-MAC mappings, MAC-to-port associations, and deviations from DHCP binding information.

In the second stage, suspicious events are evaluated by a supervised classification module trained on labeled samples from normal traffic and the three defined attack scenarios. The classifier uses the extracted feature vectors to distinguish between benign behavior and ARP spoofing-based MitM activity. The training dataset includes samples collected during the baseline phase and during Scenario A, Scenario B, and Scenario C. The dataset is divided into training and testing subsets to evaluate the model on traffic samples not used during training.

The AI decision is not used as a standalone blocking mechanism. Instead, it is correlated with DAI events and infrastructure-level indicators. A high-confidence alert is generated when the AI module detects anomalous behavior and this behavior is supported by one or more protocol-level indicators, such as unexpected IP-to-MAC mapping changes, inconsistencies with DHCP bindings, or abnormal MAC-to-port transitions. This correlation reduces the risk of false positives compared with AI-only detection and improves sensitivity compared with DAI-only protection.

The evaluation considered three configurations:

- DAI-only, where detection and prevention rely exclusively on the switch-based DAI mechanism;
- AI-only, where only the NIDS/AI module is active, without DAI enforcement;
- DAI+AI, which represents the proposed hybrid architecture.

When high-risk activity is detected, the system generates an alert and stores a forensic pcap snapshot for subsequent analysis. Under very high confidence conditions, a temporary response may also be applied, such as temporary port shutdown or a temporary DAI ACL, in accordance with a human-in-the-loop policy.

E. Evaluation Metrics and Reproducibility

The effectiveness of the evaluated configurations was assessed using the following metrics: Precision, Recall, F1-score, ROC-AUC, time-to-detect, and the number of false positives per 1000 hosts per day. These metrics were selected in order to jointly assess classification quality, operational responsiveness, and practical deployability.

All experiments were conducted in an isolated environment and documented through stored pcap files, DAI logs, DHCP binding records, and MAC-to-port history records. This allows the same traffic traces to be replayed and reanalyzed under different detection configurations, improving reproducibility and forensic traceability. The main experimental sequence consists of baseline traffic collection, execution of the defined ARP spoofing scenario, feature extraction over 60 s and 300 s observation windows, and evaluation of the DAI-only, AI-only, and DAI+AI configurations.

However, it should be noted that the laboratory setup does not fully reproduce the complexity of real enterprise networks, where larger host populations, heterogeneous services, multiple VLANs, and dynamic background traffic may affect ARP and DHCP behavior. Therefore, the reported results should be interpreted as an experimental validation of the proposed approach rather than a complete assessment for all possible production environments. Future work will include validation in larger-scale and more heterogeneous LAN environments.

III. RESULT AND DISCUSSION

A. Quantitative Performance Across Attack Scenarios

To evaluate the proposed system, a series of experiments was conducted in a controlled environment using three attack scenarios: (A) classic high-rate ARP spoofing, (B) low-rate stealth spoofing, and (C) insider spoofing. Each configuration was replicated ten times, with twenty attack injections per replication, resulting in a total of 200 injections per scenario. The performance of DAI-only, AI-only, and DAI+AI was assessed using the metrics Precision, Recall, F1-score, and ROC-AUC. The aggregated results are presented in Table 1.

TABLE 1 CLASSIFICATION PERFORMANCE ACROSS ATTACK SCENARIOS

Scenario	Configuration	Precision	Recall	F1-score	ROC-AUC
A (classic)	DAI-only	0.99 ±0.01	0.98 ±0.02	0.985 ±0.01	0.995 ±0.003
	AI-only	0.96 ±0.02	0.99 ±0.01	0.975 ±0.01	0.992 ±0.004
	DAI + AI	0.98 ±0.01	0.995 ±0.005	0.987 ±0.006	0.998 ±0.002
B (low-rate)	DAI-only	0.92 ±0.03	0.18 ±0.07	0.30 ±0.08	0.60 ±0.04
	AI-only	0.88 ±0.04	0.93 ±0.03	0.905 ±0.03	0.95 ±0.02
	DAI + AI	0.90 ±0.03	0.95 ±0.02	0.925 ±0.02	0.965 ±0.015
C (insider)	DAI-only	0.95 ±0.02	0.30 ±0.05	0.45 ±0.06	0.62 ±0.05
	AI-only	0.85 ±0.04	0.91 ±0.03	0.88 ±0.03	0.93 ±0.03
	DAI + AI	0.90 ±0.03	0.93 ±0.02	0.915 ±0.02	0.95 ±0.02

As shown in Table 1, under Scenario A, all three configurations achieved high classification performance. The DAI-only setup reached Precision of 0.99 ± 0.01 ,

Recall of 0.98 ± 0.02 , and F1-score of 0.985 ± 0.01 , confirming the strong effectiveness of DAI against conventional high-rate ARP spoofing. The AI-only configuration achieved comparable results, while the hybrid DAI+AI approach provided the highest overall values, including Recall of 0.995 ± 0.005 and ROC-AUC of 0.998 ± 0.002 . These results indicate that, in clearly expressed attack conditions, DAI already performs very well, and AI contributes only a limited additional gain.

A different pattern can be observed for Scenario B. As indicated in Table 1, DAI-only preserved relatively high Precision (0.92 ± 0.03), but its Recall dropped to 0.18 ± 0.07 and F1-score to 0.30 ± 0.08 . In contrast, AI-only achieved Recall of 0.93 ± 0.03 and F1-score of 0.905 ± 0.03 , while DAI+AI further improved Recall to 0.95 ± 0.02 and F1-score to 0.925 ± 0.02 . This confirms that low-rate spoofing can bypass conventional rule-based inspection more easily, whereas behavioral analysis remains sensitive to temporally distributed anomalies.

A similar trend was observed in Scenario C. According to Table 1, DAI-only achieved Recall of only 0.30 ± 0.05 and F1-score of 0.45 ± 0.06 , whereas AI-only reached Recall of 0.91 ± 0.03 and F1-score of 0.88 ± 0.03 . The hybrid DAI+AI configuration again provided the best overall balance, with Recall of 0.93 ± 0.02 , F1-score of 0.915 ± 0.02 , and ROC-AUC of 0.95 ± 0.02 . These results suggest that the combination of infrastructure-based validation and AI-driven behavioral analysis is particularly beneficial for insider-like or context-dependent attack patterns.

B. Detection Latency and Operational Indicators

In addition to classification metrics, the operational performance of the evaluated configurations was assessed using median time-to-detect, false positives per 1000 hosts per day, inference latency, and average CPU utilization of the AI host. These results are summarized in Table 2.

The false positive values are reported as normalized estimates per 1000 hosts/day to support comparison with operational network monitoring practice.

As shown in Table 2, for Scenario A, DAI-only achieved a median time-to-detect of 8 ± 3 s and only 0.5 ± 0.2 false positives per 1000 hosts/day. The AI-only configuration required 12 ± 4 s and produced 6 ± 1.5 false positives, while DAI+AI maintained a fast response time of 9 ± 3 s and reduced false positives to 2 ± 0.6 . This indicates that, even when AI is introduced, the hybrid architecture preserves near-real-time responsiveness while improving alert selectivity.

For Scenario B, DAI-only did not provide timely detection, as the median time-to-detect exceeded 300 s and some attacks remained unnoticed. In contrast, AI-only reduced detection latency to 180 ± 40 s, while DAI+AI further reduced it to 160 ± 35 s. At the same time, the number of false positives decreased from 7 ± 2 in AI-only to 3.5 ± 1 in DAI+AI, demonstrating that the hybrid approach improves both responsiveness and operational usability.

Under Scenario C, DAI-only required 250 ± 60 s for detection, whereas AI-only and DAI+AI reduced this value to 45 ± 15 s and 40 ± 12 s, respectively. As also indicated in Table 2, the hybrid configuration generated fewer false positives than AI-only. The inference latency of the AI module remained in the 120–160 ms range, and average CPU utilization varied between 14% and 19%, suggesting that the proposed system remains lightweight enough for practical deployment in a monitored LAN environment.

TABLE 2 DETECTION LATENCY AND OPERATIONAL METRICS

Scenario	Configuration	Median Time-to-Detect (s)	False Positives per 1000 Hosts/Day	Inference Latency (ms)	CPU Utilization (%)
A (classic)	DAI-only	8 ± 3	0.5 ± 0.2	—	—
	AI-only	12 ± 4	6 ± 1.5	120 ± 20	$14\% \pm 3$
	DAI + AI	9 ± 3	2 ± 0.6	130 ± 25	$16\% \pm 3$
B (low-rate)	DAI-only	>300 (many undetected)	0.2 ± 0.1	—	—
	AI-only	180 ± 40	7 ± 2	150 ± 30	$18\% \pm 4$
	DAI + AI	160 ± 35	3.5 ± 1	160 ± 30	$19\% \pm 4$
C (insider)	DAI-only	250 ± 60	0.3 ± 0.1	—	—
	AI-only	45 ± 15	8 ± 2	140 ± 25	$17\% \pm 3$
	DAI + AI	40 ± 12	3 ± 1	150 ± 28	$18\% \pm 3$

C. Statistical Significance of the Improvement

To verify whether the observed improvement was statistically meaningful, a paired t-test was applied to the ten replications comparing DAI-only and DAI+AI. For Scenarios B and C, the hybrid configuration showed statistically significant improvement with $p < 0.01$. For Scenario A, the difference was limited and did not consistently reach statistical significance ($p > 0.05$). This result is expected, since DAI already performs very strongly under classic high-rate attack conditions. Therefore, the main added value of the proposed hybrid architecture lies not in replacing DAI where it is already sufficient, but in strengthening detection under stealthy and insider-like conditions.

D. Forensic Observation and DAI Behavior

A representative forensic example was obtained during one of the replications of Scenario A, where a Telnet session was successfully intercepted and credentials were exposed in clear text. As illustrated in Fig. 4, the ARP spoofing attack enabled the attacker-controlled host to record traffic and recover login credentials from the captured pcap. This observation demonstrates the practical consequences of MitM attacks in the presence of unencrypted application-layer protocols.

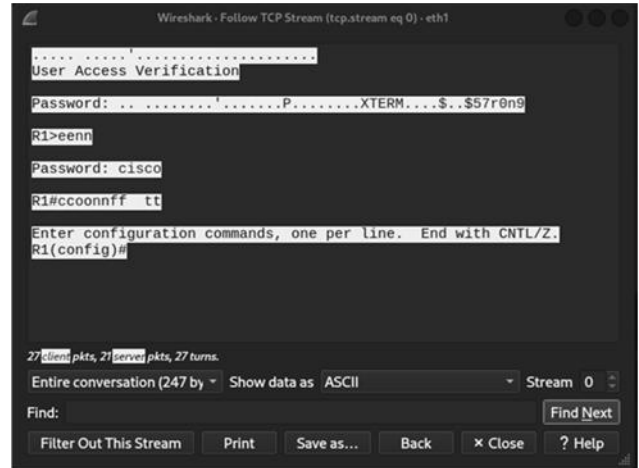


Fig. 4. Captured Telnet credentials during MitM attack.

At the same time, DAI produced %SW_DAI-4-ACL_DENY log entries indicating blocked attempts to inject invalid ARP packets. As shown in Fig. 5, these logs confirm that DAI effectively mitigates classic spoofing attempts at switch level. In parallel, the AI module detected supporting anomalies, including increased values of gratuitous_count and ip_mac_change_count, enabling the generation of a SIEM event and the automatic preservation of a forensic pcap snapshot. This combined behavior illustrates the complementary nature of the proposed architecture: DAI provides immediate infrastructure-level enforcement, while AI adds contextual awareness and analytical depth.

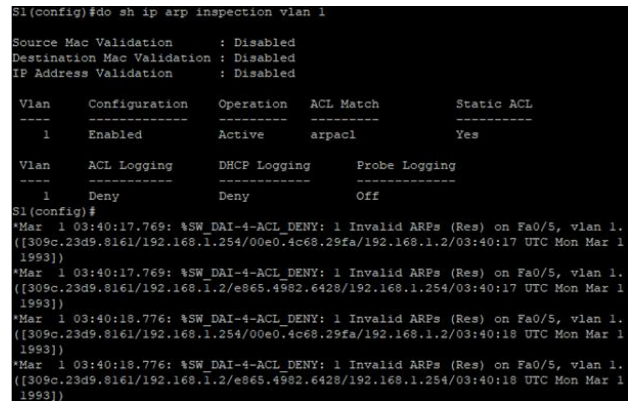


Fig. 5. DAI logs for invalid ARP packet blocking.

E. Overall Interpretation

Taken together, the results from Table 1, Table 2, Fig. 4, and Fig. 5 show that DAI-only is highly effective against classic high-frequency ARP spoofing attacks but offers limited sensitivity in low-rate and insider scenarios. The AI-only configuration substantially improves Recall and reduces detection latency in these harder cases, but at the cost of a higher false positive rate. The proposed DAI+AI architecture provides the best overall balance between detection capability, alert precision, and operational practicality.

These findings support the central assumption of the study: traditional rule-based protections remain valuable as a first line of defense, but they can be significantly strengthened through AI-based behavioral analysis. Rather than replacing DAI, the proposed system extends its effectiveness by detecting attack patterns that are formally plausible from a protocol perspective but anomalous when viewed in behavioral and temporal context.

Compared with purely rule-based ARP protection mechanisms, the proposed hybrid configuration preserves the low false positive rate and immediate enforcement capability of infrastructure-level defenses, while improving sensitivity in low-rate and insider-like attack scenarios. Compared with standalone AI-based intrusion detection, the DAI+AI configuration reduces the false positive rate by correlating behavioral anomalies with protocol-level and infrastructure-level evidence. Therefore, the proposed approach should be viewed as a complementary security layer rather than a replacement for existing ARP inspection, IDS/IPS, or anomaly detection mechanisms.

It should also be emphasized that the results represent a controlled laboratory validation of the proposed architecture. Although the attack scenarios reproduce realistic ARP-based MitM behavior, the environment is smaller and more deterministic than a production enterprise network. In larger deployments, additional factors such as multiple VLANs, higher traffic diversity, dynamic host mobility, and legitimate changes in IP-to-MAC or MAC-to-port associations may influence both detection accuracy and false positive rates. For this reason, future validation in larger and more heterogeneous LAN environments is necessary.

IV. CONCLUSIONS

This study addressed the problem of Man-in-the-Middle (MitM) protection in local area networks, with particular emphasis on ARP spoofing as one of the most common practical realizations of such attacks in IPv4 environments. A hybrid defense architecture combining Dynamic ARP Inspection (DAI) and an AI-based behavioral detection module was designed and evaluated in a controlled laboratory environment. The results demonstrate that this combined approach improves the detection of attack patterns that are difficult to identify using infrastructure-level rule enforcement alone.

The experimental findings confirm that DAI, when used as a standalone mechanism, is highly effective against classic high-rate ARP spoofing attacks, where invalid ARP behavior is explicit and can be blocked directly at switch level. However, its performance decreases substantially in low-rate stealth and insider-like scenarios, where malicious activity is more subtle, temporally distributed, or generated by a host with seemingly legitimate network presence. In these cases, the AI-based module provides a clear advantage by analyzing behavioral, statistical, and temporal relationships across ARP, DHCP, and switch-port events.

The comparison of DAI-only, AI-only, and DAI+AI shows that the hybrid configuration achieves the best overall balance between Recall, Precision, F1-score, time-

to-detect, and false positive rate. In addition to improving detection performance, the proposed approach preserves operational practicality by maintaining low inference latency and moderate computational overhead. The forensic observations further illustrate that timely detection of MitM activity is not only a matter of metric improvement, but also of preventing real exposure of sensitive information in poorly protected communication sessions.

The main contribution of this work lies in the design and experimental validation of a hybrid LAN protection model that integrates infrastructure-based ARP validation with AI-driven behavioral analysis in a single detection and response workflow. While the general combination of AI and rule-based security mechanisms is already known, the contribution of this study is the targeted application of this concept to ARP spoofing-based MitM detection and the experimental comparison of DAI-only, AI-only, and DAI+AI configurations under controlled LAN attack scenarios. The results indicate that artificial intelligence is most effective when used not as a replacement for conventional network security mechanisms, but as an adaptive extension that enhances contextual awareness and resilience against stealthy attack behavior.

At the same time, the study has several limitations. The experiments were conducted in a controlled laboratory environment and therefore do not fully capture the complexity of large-scale production networks with heterogeneous services, dense background traffic, and multiple simultaneous anomalies. In addition, the evaluation focused specifically on ARP-based MitM attacks, which means that the reported results should not be generalized directly to other forms of MitM, such as DNS spoofing or TLS-related interception attacks.

Future work should therefore focus on validating the proposed approach in larger and more diverse network environments, extending the feature set with additional telemetry sources, and incorporating explainable AI mechanisms to improve the transparency of detection decisions. Further research may also explore adaptive response strategies in which the system recommends mitigation actions according to risk level and a predefined human-in-the-loop policy, while avoiding fully automated blocking decisions in ambiguous cases.

REFERENCES

- [1] C. Surianarayanan, "Integration of the Internet of Things and Cloud: Security Challenges and Solutions – A Review," *International Journal of Cloud Applications and Computing*, vol. 13, pp. 1–30, Mar. 2023, doi: [10.4018/IJCAAC.325624](https://doi.org/10.4018/IJCAAC.325624).
- [2] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," *SECURITY AND PRIVACY*, vol. 8, no. 2, p. e70016, Mar. 2025, doi: [10.1002/spy2.70016](https://doi.org/10.1002/spy2.70016).
- [3] D. C. Plummer, "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," Nov. 1982, doi: [10.17487/rfc0826](https://doi.org/10.17487/rfc0826).
- [4] S. Y. Nam, S. Jurayev, S. S. Kim, K. Choi, and G. S. Choi, "Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN," *EURASIP Journal on Wireless Communications and Networking* 2012 2012:1, vol. 2012, no. 1, pp. 89–, Mar. 2012, doi: [10.1186/1687-1499-2012-89](https://doi.org/10.1186/1687-1499-2012-89).

- [5] D. Hanna, P. Veeraraghavan, and E. Pardede, "PrECast: An Efficient Crypto-Free Solution for Broadcast-Based Attacks in IPv4 Networks," *Electronics* 2018, Vol. 7, Page 65, vol. 7, no. 5, p. 65, May 2018, doi: [10.3390/electronics7050065](https://doi.org/10.3390/electronics7050065).
- [6] Z. Shah and S. Cosgrove, "Mitigating ARP Cache Poisoning Attack in Software-Defined Networking (SDN): A Survey," *Electronics* 2019, Vol. 8, Page 1095, vol. 8, no. 10, p. 1095, Sep. 2019, doi: [10.3390/electronics8101095](https://doi.org/10.3390/electronics8101095).
- [7] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions," *Electronics* 2020, Vol. 9, Page 1177, vol. 9, no. 7, p. 1177, Jul. 2020, doi: [10.3390/electronics9071177](https://doi.org/10.3390/electronics9071177).
- [8] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," *Measurement: Sensors*, vol. 28, p. 100827, Aug. 2023, doi: [10.1016/j.measen.2023.100827](https://doi.org/10.1016/j.measen.2023.100827).
- [9] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, Oct. 2017, doi: [10.1109/ACCESS.2017.2762418](https://doi.org/10.1109/ACCESS.2017.2762418).
- [10] P. Schummer, A. del Rio, J. Serrano, D. Jimenez, G. Sánchez, and Á. Llorente, "Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation," *AI* 2024, Vol. 5, Pages 2967-2983, vol. 5, no. 4, pp. 2967–2983, Dec. 2024, doi: [10.3390/ai5040143](https://doi.org/10.3390/ai5040143).
- [11] R. Chinnnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, "Deep learning-driven methods for network-based intrusion detection systems: A systematic review," *ICT Express*, vol. 11, no. 1, pp. 181–215, Feb. 2025, doi: [10.1016/j.ict.2025.01.005](https://doi.org/10.1016/j.ict.2025.01.005).
- [12] M. M. Alani, A. I. Awad, and E. Barka, "ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning," *Internet of Things*, vol. 23, p. 100861, Oct. 2023, doi: [10.1016/j.iot.2023.100861](https://doi.org/10.1016/j.iot.2023.100861).
- [13] K. Sauka, G. Y. Shin, D. W. Kim, and M. M. Han, "Adversarial Robust and Explainable Network Intrusion Detection Systems Based on Deep Learning," *Applied Sciences* 2022, Vol. 12, Page 6451, vol. 12, no. 13, p. 6451, Jun. 2022, doi: [10.3390/app12136451](https://doi.org/10.3390/app12136451).
- [14] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Inf. Sci. (N. Y.)*, vol. 639, no. 10, p. 119000, Aug. 2023, doi: [10.1016/j.ins.2023.119000](https://doi.org/10.1016/j.ins.2023.119000).
- [15] M. M. Issa, M. Aljanabi, and H. M. Muhialdeen, "Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations," *Journal of Intelligent Systems*, vol. 33, no. 1, Jan. 2024, doi: [10.1515/jisys-2023-0248](https://doi.org/10.1515/jisys-2023-0248).

Performance and Resilience Analysis of GRE over IPsec Tunnels in Dynamic Routing Networks

Penka Markova

Computer Science and Engineering
Technical University of Varna
Varna, Bulgaria
penkamarkova5@gmail.com

Georgi Markov

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
g.markov@naval-acad.bg

Abstract— This paper presents the design and experimental evaluation of Generic Routing Encapsulation over Internet Protocol Security tunnels in dynamic routing networks. The study is motivated by the need to provide secure inter site connectivity while preserving support for dynamic route exchange between remote network segments. A laboratory topology is developed to examine the behavior of the proposed tunnel architecture under normal operation and during network failures. The evaluation focuses on key indicators including throughput, delay, jitter, packet loss, and routing convergence time. In addition, resilience is assessed through controlled disruption and recovery scenarios in order to measure tunnel stability, service continuity, and network reconvergence. The results are used to analyze the balance between secure communication and the performance impact introduced by encapsulation and tunnel protection. Particular attention is given to the practical suitability of this approach for distributed networks that require both protected traffic transmission and flexible routing operation. The study shows that GRE over IPsec remains an effective solution for secure dynamic routing environments when performance limitations and recovery characteristics are properly considered in network design and deployment.

Keywords— dynamic routing protocols, GRE over IPsec, resilience analysis, routing convergence, secure inter-site connectivity, tunnel performance.

I. INTRODUCTION

Modern distributed networks are often required to exchange routing information across geographically separated sites while maintaining confidentiality, integrity, and controlled access to operational traffic. In such environments, secure site-to-site connectivity must support not only data forwarding but also the reliable operation of the routing control plane. Internet Protocol Security (IPsec) is a widely adopted framework for protecting IP communications by providing confidentiality, integrity,

authentication, and anti-replay protection [1]. At the same time, Generic Routing Encapsulation (GRE) offers a flexible mechanism for transporting network-layer traffic over an overlay tunnel [2]. When these two technologies are combined, it becomes possible to build secure logical links that also preserve support for dynamic routing protocols.

This combination is especially relevant in networks where redundancy, topology changes, and automatic path recovery must be supported without frequent manual intervention. Dynamic routing protocols such as OSPF rely on the continuous exchange of control messages and on the logical visibility of routed paths between remote sites [3]. GRE over IPsec provides a practical means of enabling such routing exchanges over protected inter-site connections, thereby making the tunnel interface appear as a normal routed link from the perspective of the routing process [4].

Despite these advantages, GRE over IPsec introduces additional encapsulation overhead and processing cost. The layered use of GRE and IPsec increases packet size, reduces effective payload efficiency, and may create sensitivity to Maximum Transmission Unit (MTU) limitations, packet fragmentation, and additional cryptographic processing [5]. These factors can influence key operational indicators such as throughput, delay, jitter, packet loss, and routing recovery behavior. As a result, the use of GRE over IPsec involves a practical trade-off between improved security and the performance penalties associated with nested tunneling and encryption.

For these reasons, this paper investigates the performance and resilience of GRE over IPsec tunnels in dynamic routing networks. Rather than proposing GRE over IPsec as a new tunneling mechanism, the study provides a controlled experimental assessment of its operational behavior when dynamic routing, encryption,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.53>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

encapsulation overhead, and link recovery are considered together. The laboratory implementation evaluates tunnel behavior during normal operation and under controlled failure and recovery conditions. The analysis focuses on throughput, delay, jitter, packet loss, and routing convergence time in order to assess the balance between communication security, routing flexibility, and operational robustness.

The main contribution of the paper is an experimentally grounded evaluation of GRE over IPsec in a reproducible laboratory scenario, with emphasis on measurable performance impact and service continuity during routing changes. The scope is intentionally limited to a compact test topology that allows the influence of tunneling, encryption, and dynamic routing behavior to be isolated. Evaluation of larger multi-site topologies and comparison with newer overlay VPN approaches are identified as directions for future work.

II. BACKGROUND AND RELATED WORK

GRE over IPsec is an established tunneling approach used when a network must combine flexible traffic encapsulation with protected inter-site communication. In this architecture, GRE performs the logical encapsulation of routed traffic, while IPsec protects the encapsulated packets during transport across the external network [4]. Therefore, the novelty of recent research in this area is not associated with the existence of the mechanism itself, but with its measured behavior under specific routing, security, and failure-recovery conditions. This layered design remains relevant in environments where dynamic routing protocols, multicast traffic, or additional protocol flexibility must be preserved across a secure tunnel [6].

The relevance of GRE over IPsec in dynamic routing environments is directly related to routing protocol support. Conventional site-to-site IPsec deployments may secure traffic successfully, but they do not always provide the same flexibility for transporting routing updates and maintaining a routed overlay between remote sites. GRE addresses this limitation by creating a logical point-to-point tunnel over which routing adjacencies can be formed and maintained [4], [7]. In this way, the combination of GRE and IPsec is well suited to distributed networks in which secure transport and dynamic route exchange must coexist.

Recent studies on overlay networking and VPN performance further support the need for experimental analysis of tunnel-based secure connectivity. Existing research shows that overlay design choices have measurable effects on round-trip time, bandwidth efficiency, and service stability [8]. Other studies have emphasized that VPN performance is strongly influenced by packet processing overhead, protocol stack behavior, and virtual interface implementation [9]. These findings are directly relevant to GRE over IPsec, where GRE encapsulation and IPsec protection operate together and therefore jointly affect communication efficiency.

A central practical issue in GRE over IPsec deployments is the impact of encapsulation overhead. The addition of GRE headers, followed by IPsec processing and protection headers, increases packet size and reduces the

proportion of useful payload in each transmitted frame. This may amplify MTU sensitivity, increase the risk of fragmentation, and degrade performance under load. Consequently, any realistic assessment of GRE over IPsec should not treat tunnel establishment as the sole success criterion, but should also evaluate the impact of the solution on throughput, delay, jitter, and packet loss [8], [9]. For reproducibility, such assessments should also specify the IPsec profile, routing protocol parameters, traffic generation method, and measurement tools, since these factors can significantly affect the observed results.

Another important aspect concerns deployment limitations and alternative overlay approaches. GRE over IPsec is typically implemented as a point-to-point solution and is subject to practical restrictions regarding scalability and session design [4]. These characteristics distinguish it from more advanced multipoint or policy-driven overlay architectures, such as DMVPN, FlexVPN, route-based IPsec/VTI deployments, WireGuard-based VPNs, and SD-WAN solutions [10]. Such technologies may offer better scalability, simplified tunnel management, or centralized policy control in larger networks. However, GRE over IPsec remains relevant in compact and medium-sized deployments because of its wide platform support, clear tunnel semantics, and compatibility with dynamic routing. For this reason, the present paper focuses on the operational behavior of GRE over IPsec itself, while a direct comparative evaluation with newer overlay VPN technologies is left for future work.

Recent work on routing resilience also justifies the focus on convergence and recovery behavior in this study. Research comparing dynamic routing protocols under failure conditions has shown that convergence time, traffic redistribution, and recovery stability are critical indicators in routed environments [11]. Similarly, recent studies involving GRE-based routing deployments have reported measurable effects on jitter, packet loss, and recovery time during link disruption [7]. These findings suggest that tunnel-based secure communication should be evaluated not only in steady state, but also during service interruption and restoration.

Based on the reviewed literature and practical platform guidance, the main research gap is not whether GRE over IPsec can provide secure routed connectivity, since this capability is already well established, but how effectively it performs and recovers under defined dynamic routing and failure conditions. The existing literature discusses tunnel overhead, VPN performance, and routing convergence, but fewer studies combine these aspects in a reproducible GRE over IPsec laboratory scenario. This gap motivates the experimental focus of the present study on performance metrics and recovery behavior in a controlled deployment.

III. MATERIALS AND METHODS

A. Testbed Topology and Network Architecture

The experimental environment was designed as a small-scale inter-site network intended to emulate secure communication between two geographically separated

local area networks connected through an external IP transport infrastructure.

This topology was intentionally kept compact in order to focus on the behavior of a single GRE over IPsec tunnel in realistic operating conditions. The design supports direct observation of traffic forwarding, routing updates, tunnel status, and recovery behavior while avoiding the additional complexity of multi-path or large-scale environments. Although the topology does not represent a large multi-site deployment, it provides a controlled environment in which the effects of GRE encapsulation, IPsec protection, and OSPF-based recovery can be isolated and measured.

The experimental topology used in the study is illustrated in Fig. 1.

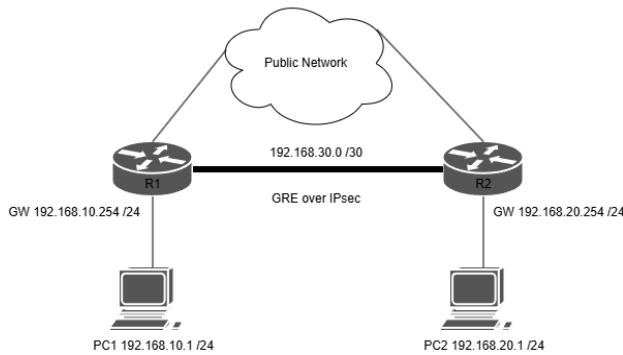


Fig. 1. Experimental topology of the GRE over IPsec inter-site testbed.

The first local segment, LAN1, contains a host with IP address 192.168.10.1/24, while the LAN-facing interface of R1 is configured with address 192.168.10.254/24. The second local segment, LAN2, contains a host with IP address 192.168.20.1/24, while the LAN-facing interface of R2 is configured with address 192.168.20.254/24. The tunnel endpoints communicate across an external IP transport network through WAN-facing interfaces. Over this transport path, a GRE tunnel is created, and IPsec is applied to protect the GRE traffic exchanged between the routers.

This topology was intentionally kept compact in order to focus on the behavior of a single GRE over IPsec tunnel in realistic operating conditions. The design supports direct observation of traffic forwarding, routing updates, tunnel status, and recovery behavior while avoiding the additional complexity of multi-path or large-scale environments.

B. GRE over IPsec Tunnel Design

The implemented tunnel architecture combines GRE and IPsec in order to preserve support for routing protocol exchange while simultaneously securing traffic across the interconnecting network. GRE serves as the logical transport mechanism between the remote routers, allowing the tunnel to carry both user-plane and control-plane traffic. IPsec provides confidentiality and integrity for the GRE-encapsulated packets transmitted over the WAN-facing path [1].

The tunnel was configured as a point-to-point logical connection between R1 and R2. From the perspective of

the routing process, the GRE interface behaves as a normal routed link, which makes it possible to establish dynamic routing adjacency across the secure overlay. This architecture reflects a practical deployment model for secure inter-site communication where traditional site-to-site IPsec alone may not provide sufficient flexibility for routing protocol transport.

The main GRE and IPsec configuration parameters used in the experiment are summarized in Table 1. These parameters were kept constant across all protected-tunnel measurements in order to ensure comparability between the traffic scenarios.

TABLE 1 GRE OVER IPSEC CONFIGURATION PARAMETERS

Parameter	Value
GRE tunnel mode	Point-to-point GRE tunnel
Tunnel source/destination	WAN-facing interfaces of R1 and R2
Tunnel addressing	Routed point-to-point tunnel subnet
Routing protocol over tunnel	OSPF
IPsec protection target	GRE traffic between R1 and R2
IKE version	IKEv2
Encryption algorithm	AES-256
Integrity / hash algorithm	SHA-256
Authentication method	Pre-shared key
Diffie-Hellman group	Group 14
IPsec mode	Tunnel mode
SA lifetime	86000

The operational state of the tunnel and the associated IPsec protection were verified on the tunnel endpoint, as shown in Fig. 2.

```
R1#sh int tunnel 1
Tunnel1 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.30.1/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.10.254 destination 192.168.20.254
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:32, output 00:00:04, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 1 packets input, 100 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
141 packets output, 14084 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 unknown protocol drops
 0 output buffer failures, 0 output buffers swapped out
R1#sh cry
R1#sh crypto se
R1#sh crypto session
Crypto session current status

Interface: GigabitEthernet0/2
Session status: UP-ACTIVE
Peer: 192.168.20.254 port 500
IKEv1 SA: local 192.168.10.254/500 remote 192.168.20.254/500 Active
IPSEC FLOW: permit 47 host 192.168.20.0/24 host 192.168.10.0/24
Active SAs: 2, origin: crypto map
```

Fig. 2. Verification of GRE tunnel status and active IPsec session on router R1.

The output confirms that the GRE tunnel interface was operational and that an active IPsec session had been established between the peers. The verification included tunnel interface status, crypto session state, encapsulated and decapsulated packet counters, and the presence of protected GRE traffic between the two WAN-facing endpoints.

C. Dynamic Routing Operation

Dynamic routing was enabled across the GRE tunnel using OSPF in order to evaluate not only basic connectivity, but also the suitability of the solution for routed inter-site operation. The OSPF configuration used a single routing area and formed adjacency over the GRE tunnel interface. The LAN networks behind R1 and R2 were advertised through OSPF, allowing end-to-end reachability to be restored automatically after tunnel recovery. The same OSPF parameters were maintained throughout the experiments in order to avoid changes in convergence behavior caused by routing configuration differences. OSPF Hello traffic was observed traversing the GRE tunnel, confirming that routing protocol exchanges were successfully carried over the protected logical path. This behavior demonstrates that the tunnel architecture supports the control plane required for adaptive routing between the two remote LAN segments.

In the context of the present study, dynamic routing is treated as a core functional property of the tunnel environment rather than as an auxiliary feature. The presence of routing protocol traffic allows the experiment to assess not only data forwarding performance, but also convergence and recovery after transport disruption.

Packet capture analysis further confirmed the presence of both routing control traffic and end-to-end user traffic in the experimental environment, as illustrated in Fig. 3.

The observed OSPF hello packets and successful ICMP exchanges support the conclusion that the tunnel carried both control-plane and user-plane traffic.

34733	145.597000	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=95/24328, ttl=126 (request in 34732)
34734	146.601547	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=96/24329, ttl=126 (reply in 34733)
34735	146.602710	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=96/24329, ttl=126 (request in 34734)
34736	147.610765	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=97/24332, ttl=126 (reply in 34737)
34737	147.611979	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=97/24332, ttl=126 (request in 34736)
34738	146.610211	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=98/25086, ttl=126 (reply in 34739)
34739	148.627248	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=98/25086, ttl=126 (request in 34738)
34740	149.641683	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=99/25344, ttl=126 (reply in 34741)
34741	149.642814	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=99/25344, ttl=126 (request in 34740)
34742	150.650997	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=100/25086, ttl=126 (reply in 34743)
34743	150.650873	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=100/25086, ttl=126 (request in 34742)
34744	151.672377	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=101/25056, ttl=126 (reply in 34745)
34745	151.673589	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=101/25056, ttl=126 (request in 34744)
34746	152.261123	192.168.20.224	0.0.5	OSPF 98 Hello Packet	
34747	152.687700	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=102/26112, ttl=126 (reply in 34748)
34748	152.688706	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=102/26112, ttl=126 (request in 34747)
34749	153.783143	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=103/26368, ttl=126 (reply in 34750)
34750	153.784942	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=103/26368, ttl=126 (request in 34749)
34751	154.718486	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=104/26624, ttl=126 (reply in 34752)
34752	154.719452	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=104/26624, ttl=126 (request in 34751)
34753	154.945290	Cisco 2d:05:58	Cisco 2d:05:58	LOOP 68 Reply	
34754	155.731866	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=105/26880, ttl=126 (reply in 34755)
34755	155.735126	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=105/26880, ttl=126 (request in 34754)
34756	156.749226	192.168.20.1	192.168.10.1	ICMP 74 Echo (ping) request	id=0x0001, seq=106/27136, ttl=126 (reply in 34757)
34757	156.750489	192.168.10.1	192.168.20.1	ICMP 74 Echo (ping) reply	id=0x0001, seq=106/27136, ttl=126 (request in 34756)

Fig. 3. Verification of GRE tunnel status and active IPsec session on router R1.

D. Measurement Metrics and Traffic Scenarios

The methodological focus of the study is not limited to successful tunnel establishment. Instead, the objective is to quantify the operational impact of layered encapsulation and encryption on network behavior. For this reason, the evaluation considers throughput, end-to-end delay, jitter,

packet loss, and routing convergence time as the main performance indicators [11], [12].

The measurements were performed using iperf3 for TCP and UDP traffic generation, ICMP echo tests for reachability and delay observation, Wireshark for packet capture analysis, and Cisco IOS diagnostic commands for tunnel, routing, and IPsec verification. Router CLI outputs were used to monitor tunnel state, OSPF adjacency, crypto session status, and encapsulation/decapsulation counters during normal operation and recovery.

The measurements are structured around several comparative traffic scenarios. First, baseline measurements are collected without tunnel protection in order to establish reference values for the underlying network path. Second, equivalent traffic is transmitted across the GRE tunnel without IPsec in order to isolate the effect of GRE encapsulation. Third, traffic is measured over the complete GRE over IPsec configuration in order to assess the additional impact of encryption and tunnel protection. This staged methodology allows the individual and combined effects of encapsulation and security processing to be interpreted more clearly.

Both TCP and UDP traffic scenarios are included in the evaluation. TCP traffic is used to examine the impact of the tunnel architecture on reliable data transfer and effective throughput, while UDP traffic is used to assess delay, jitter, and packet loss under controlled offered load. This combination provides a balanced view of tunnel performance for both connection-oriented and real-time traffic patterns.

The measurements are reported as representative observations obtained under stable laboratory conditions. Since the experiments were performed in a controlled environment with fixed topology, fixed configuration parameters, and limited background traffic, the results are suitable for comparative interpretation within the tested scenario. However, repeated measurements over longer observation periods would be required for stronger statistical generalization.

E. Failure and Recovery Procedure

In addition to performance measurements, the study includes a resilience assessment under failure conditions. Controlled disruption is introduced at the WAN-facing side of the tunnel environment in order to observe the response of the protected tunnel, the routing process, and end-to-end communication. The recovery phase is then monitored in order to determine the time required for restoration of the IPsec security association, re-establishment of the GRE tunnel, recovery of OSPF adjacency, and stabilization of user traffic.

The disruption was introduced by administratively disabling the WAN-facing interface, and recovery was initiated by restoring the same interface. The recovery interval was measured from the moment of transport restoration until stable end-to-end communication between LAN1 and LAN2 was observed again. During this interval, tunnel state, IPsec session state, OSPF adjacency, and user traffic restoration were monitored.

This procedure makes it possible to distinguish between several different phases of recovery: transport restoration, tunnel restoration, routing reconvergence, and traffic stabilization [11]. Such separation is important because a tunnel may return to the up state before communication quality fully returns to steady-state conditions.

F. Scope and Limitations

The developed topology is intentionally limited to a single protected logical path between two routers. As a result, the resilience analysis in this paper focuses on service continuity, tunnel recovery, and routing reconvergence rather than on redundancy-based failover through alternative underlay links. The study therefore addresses operational resilience in the sense of automatic recovery after transient interruption, but not high-availability behavior based on path diversity.

Within this scope, the main methodological contribution of the study is the combined evaluation of performance and recovery behavior in a dynamic routing environment using GRE over IPsec. The experimental design provides a practical basis for assessing the suitability of this architecture for secure routed inter-site communication. A direct performance comparison with DMVPN, FlexVPN, VTI-based IPsec, WireGuard, or SD-WAN overlays is outside the scope of the present study and is considered future work.

IV. RESULTS AND DISCUSSION

A. Performance Assessment

The results obtained in the laboratory network environment show that GRE over IPsec provides stable and functionally correct communication between the two remote LAN segments under the tested conditions. The tunnel successfully carries both user-plane and control-plane traffic, including OSPF exchanges, thereby confirming its suitability for routed inter-site operation in the evaluated topology.

At the same time, the measurements clearly indicate that the use of GRE encapsulation and IPsec protection introduces measurable communication overhead. Compared with plain IP forwarding, the protected tunnel produces lower effective throughput, increased delay, higher jitter, and a slight increase in packet loss. These effects are consistent with the additional header overhead and processing requirements imposed by GRE and IPsec.

The comparative scenarios also show that GRE alone introduces a moderate performance cost, while the full GRE over IPsec configuration results in the most visible degradation. This confirms that the additional headers, encryption, integrity protection, and cryptographic processing associated with IPsec contribute significantly to the total performance impact of the architecture. From an engineering perspective, the findings demonstrate that secure tunneling should be evaluated not only in terms of functionality, but also in terms of transport efficiency and service quality under expected traffic load.

The reported values should be interpreted as representative measurements obtained under stable laboratory conditions with fixed topology, fixed configuration parameters, and limited background traffic. The detailed numerical results for TCP and UDP traffic are presented in the corresponding tables:

TABLE 2 RESULTS FOR TCP TRAFFIC

Operating mode	Average throughput (Mbps)
No tunnel	94.8
GRE without IPsec	91.6
GRE over IPsec	84.9

TABLE 3 RESULTS FOR UDP TRAFFIC AT 20 MBPS OFFERED LOAD

Operating mode	Actual received traffic (Mbps)	Average delay (ms)	Jitter (ms)	Packet loss (%)
No tunnel	19.98	3.3	0.42	0.0
GRE without IPsec	19.74	4.4	0.71	0.3
GRE over IPsec	18.92	6.8	1.36	1.2

TABLE 4 RELATIVE IMPACT COMPARED WITH PLAIN IP FORWARDING FOR TCP TRAFFIC

Metric	GRE without IPsec	GRE over IPsec
Throughput reduction	3.4%	10.4%
RTT increase	29.0%	100.0%
Jitter increase	56.7%	193.3%
Packet loss increase	+0.1 percentage points	+0.4 percentage points

B. Resilience Assessment

The resilience assessment shows that disruption of the WAN-facing interface leads to an almost immediate interruption of end-to-end communication, followed by loss of the protected tunnel and interruption of routing continuity. The recovery times were derived from the observed event timestamps, router diagnostic outputs, OSPF adjacency state changes, IPsec session status, and end-to-end ICMP reachability. The first failed ping is observed approximately 0.1 s after the interruption, the GRE tunnel enters a down state after about 1.0 s, and OSPF adjacency is lost after about 1.1 s. This confirms that both tunnel availability and routing continuity are directly dependent on the availability of the underlying transport path.

After restoration of the WAN interface, the IPsec security association is re-established within approximately 3.6 s, the GRE tunnel returns to the up/up state after about 4.3 s, and OSPF reaches FULL state after approximately 6.8 s. The total communication outage lasts approximately 14.9 s from the beginning of the disruption, while full service stabilization is achieved approximately 18.0 s after the disruption starts. These results indicate that the implemented GRE over IPsec solution is resilient in the sense of automatic service recovery after temporary failure, although it does not provide path redundancy through an alternative underlay route.

An additional observation concerns post-recovery stability. Although the tunnel becomes operational again within a relatively short interval, communication quality does not immediately return to its steady-state baseline. A short post-recovery phase is observed in which jitter remains elevated and packet loss temporarily increases. This indicates that tunnel restoration, routing reconvergence, and traffic stabilization should be treated as distinct but related phases of recovery.

The resilience-related measurements are summarized in the following tables:

TABLE 5 EVENT TIMELINE DURING CONTROLLED DISRUPTION AND RECOVERY

Event	Time from test start (s)
Normal operation	0–30.0 s
WAN interface disabled on R1	30.0 s
First failed ping	30.1 s
IPsec session begins to fail	30.4 s
GRE tunnel enters down state	31.0 s
OSPF adjacency lost	31.1 s
WAN interface restored	38.0 s
IPsec re-established	41.6 s
GRE tunnel up/up	42.3 s
OSPF adjacency FULL	44.8 s
First successful ping after recovery	45.0 s
Communication stabilized	48.0 s

TABLE 6 MEASURED RESILIENCE INDICATORS

Indicator	Value
Start of disruption	30.0 s
Duration of physical interruption	8.0 s
Time until tunnel failure	1.0 s
Time until OSPF adjacency loss	1.1 s
Time to IPsec re-establishment	3.6 s after link restoration
Time to GRE tunnel recovery	4.3 s after link restoration
Time to OSPF recovery	6.8 s after link restoration
Total communication outage	14.9 s
Time to full service stabilization	18.0 s

TABLE 7 TRAFFIC BEHAVIOR BEFORE, DURING, AND AFTER DISRUPTION

Metric	Before disruption	During disruption	After recovery
TCP throughput	84.9 Mbps	0 Mbps	82.7 Mbps
UDP received rate	18.92 Mbps	0 Mbps	18.45 Mbps
RTT	6.2 ms	timeout	7.1 ms
Jitter	0.88 ms	—	1.94 ms
Packet loss	0.4%	100%	2.8% during first 5 s
OSPF state	FULL	DOWN	FULL

These resilience results are specific to the tested configuration, routing timers, IPsec parameters, router platform, and failure procedure. Therefore, they should not be interpreted as universal recovery times for all GRE over IPsec deployments. Instead, they demonstrate the sequence of recovery phases and the type of operational impact that

may occur when the protected underlay path is temporarily interrupted.

C. Discussion of Trade-Offs

Taken together, the results show that GRE over IPsec provides a practical and functionally effective solution for secure communication in networks that require dynamic route exchange between remote sites. The architecture successfully supports both data forwarding and routing control traffic, thereby preserving routing flexibility while securing the communication path.

However, this functional advantage is accompanied by measurable performance cost. The combined use of GRE encapsulation and IPsec protection reduces effective throughput, increases delay and jitter, and introduces a modest increase in packet loss compared with plain forwarding. In addition, temporary underlay failure causes complete service interruption, followed by a recovery interval during which the cryptographic session, tunnel state, and routing adjacency must all be restored before traffic fully stabilizes.

These findings suggest that GRE over IPsec should be regarded as a solution that offers an effective balance between security and routing flexibility rather than maximum transport efficiency. In practical deployments, this makes the architecture well suited for protected inter-site communication where moderate performance trade-offs are acceptable. At the same time, the expected recovery interval and short-term post-recovery instability should be considered carefully in networks that carry delay-sensitive traffic or require strict service continuity.

The results also indicate that GRE over IPsec remains a practical solution when dynamic routing support and broad platform compatibility are required, but it should not be considered the only possible secure overlay design. Technologies such as DMVPN, FlexVPN, VTI-based IPsec, WireGuard-based VPNs, and SD-WAN overlays may provide advantages in scalability, centralized policy management, or multipoint connectivity. A direct experimental comparison with these alternatives is outside the scope of the present paper and is identified as future work.

From a practical design perspective, the obtained results suggest that GRE over IPsec is appropriate for controlled inter-site deployments where secure routing exchange is required and where a moderate reduction in throughput and increase in delay can be accepted. For larger networks, delay-sensitive services, or strict high-availability requirements, additional mechanisms such as redundant underlay paths, optimized MTU settings, tuned routing timers, or alternative overlay VPN architectures should be considered.

V. CONCLUSIONS

This paper presented the design, implementation, and experimental evaluation of a GRE over IPsec tunnel in a dynamic routing environment connecting two remote LAN segments through an external IP transport network. The study did not aim to introduce GRE over IPsec as a new tunneling mechanism, since this approach is already well

established. Instead, the contribution of the paper is a controlled laboratory assessment of its performance and recovery behavior when GRE encapsulation, IPsec protection, and OSPF-based dynamic routing are used together.

The practical implementation confirmed that the combined use of GRE and IPsec makes it possible to maintain secure inter-site communication while preserving the exchange of routing control traffic across the tunnel. The tunnel successfully carried both user-plane and control-plane traffic, including OSPF messages, thereby demonstrating its suitability for the evaluated scenario, where protected communication and routing flexibility were both required.

At the same time, the experimental results showed that GRE over IPsec introduces measurable communication overhead. Compared with plain IP forwarding, the protected tunnel resulted in lower effective throughput, increased delay, higher jitter, and a slight increase in packet loss. These effects became more pronounced when IPsec protection was applied on top of GRE, confirming that additional encapsulation, security headers, and cryptographic processing contribute significantly to the total performance impact.

The resilience evaluation further demonstrated that temporary loss of the underlay connection causes immediate interruption of communication, loss of tunnel availability, and disruption of routing continuity. Nevertheless, after restoration of the transport path, the IPsec security association, GRE tunnel state, and OSPF adjacency were re-established automatically without manual intervention. This confirms that the implemented architecture is resilient in the sense of service recovery after transient failure, even though it does not provide redundancy-based failover through alternative paths. The results also showed that communication quality does not return instantly to steady-state conditions after restoration, since a short post-recovery phase with elevated jitter and temporary packet loss was observed.

From a practical perspective, the findings indicate that GRE over IPsec remains a viable solution for secure communication in dynamic routing networks when both traffic protection and routing functionality are required across remote sites. However, the results should be interpreted within the limits of the tested topology, router platform, traffic scenarios, OSPF parameters, and IPsec configuration. The architecture offers an effective balance between security and operational flexibility, but its deployment should be accompanied by prior assessment of the expected impact on traffic quality, MTU behavior, and recovery time.

The main limitation of the present study is the scale of the experimental environment. Because the implementation was based on a single protected logical path between two routers, the work addresses performance and recovery-oriented resilience rather than redundancy-based failover or large-scale overlay behavior. In addition, the study does not provide a direct comparison with newer

or more scalable VPN and overlay approaches such as DMVPN, FlexVPN, VTI-based IPsec, WireGuard-based VPNs, or SD-WAN solutions.

Future work may extend the evaluation toward more complex topologies involving multiple tunnels, redundant WAN paths, larger numbers of routing nodes, comparative routing protocol analysis, optimized MTU and timer settings, and repeated long-duration measurements. A direct experimental comparison with alternative secure overlay technologies would also provide a broader basis for evaluating the trade-offs between security, scalability, routing flexibility, and recovery performance.

In conclusion, the experimental evidence supports the view that GRE over IPsec is an effective and operationally relevant solution for secure routed communication between remote network segments in controlled inter-site deployments. Although the approach introduces measurable overhead and temporary degradation during recovery, it continues to provide a practical combination of traffic protection and routing support when its performance and resilience limitations are properly considered.

REFERENCES

- [1] K. Seo and S. Kent, "Security Architecture for the Internet Protocol," Dec. 2005, *RFC Editor*. doi: [10.17487/RFC4301](https://doi.org/10.17487/RFC4301).
- [2] T. Li, D. Farinacci, S. P. Hanks, D. Meyer, and P. S. Traina, "Generic Routing Encapsulation (GRE)," Mar. 2000, *RFC Editor*. doi: [10.17487/RFC2784](https://doi.org/10.17487/RFC2784).
- [3] J. Moy, "OSPF Version 2," Apr. 1998, *RFC Editor*. doi: [10.17487/RFC2328](https://doi.org/10.17487/RFC2328).
- [4] Cisco, "Security Configuration Guide, Cisco IOS XE 17.14.x (Catalyst 9300 Switches) - Configuring GRE over IPsec ." Accessed: Apr. 07, 2026. [Online]. Available: https://web.archive.org/web/20260407185156/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-14/configuration_guide/sec/b_1714_sec_9300_cg/configuring_gre_over_ipsec.html
- [5] P. Savola, "MTU and Fragmentation Issues with In-the-Network Tunneling," Apr. 2006, *RFC Editor*. doi: [10.17487/RFC4459](https://doi.org/10.17487/RFC4459).
- [6] Cisco, "Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - GRE Over IPsec Tunnels." Accessed: Apr. 08, 2026. [Online]. Available: <https://web.archive.org/web/20260407190810/https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-gre-over-ipsec-tunnels.html>
- [7] M. Huda and W. Andriyani, "Multi-Area OSPF Analysis Using Virtual Link and GRE Tunnel," *Eduvest - Journal of Universal Studies*, vol. 5, no. 2, pp. 1804–1819, Feb. 2025, doi: [10.59188/EDUVEST.V5I2.1710](https://doi.org/10.59188/EDUVEST.V5I2.1710).
- [8] A. F. Gentile, D. Macri, E. Greco, and P. Fazio, "Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment," *Future Internet* 2024, Vol. 16, Page 283, vol. 16, no. 8, p. 283, Aug. 2024, doi: [10.3390/FI16080283](https://doi.org/10.3390/FI16080283).
- [9] C. Fu *et al.*, "A Generic High-Performance Architecture for VPN Gateways," *Electronics* 2024, Vol. 13, Page 2031, vol. 13, no. 11, p. 2031, May 2024, doi: [10.3390/ELECTRONICS13112031](https://doi.org/10.3390/ELECTRONICS13112031).
- [10] J. Dudczyk, M. Sergiel, and J. Krygier, "Analysis of SD-WAN Architectures and Techniques for Efficient Traffic Control Under Transmission Constraints—Overview of Solutions," *Sensors* 2025, Vol. 25, Page 6317, vol. 25, no. 20, p. 6317, Oct. 2025, doi: [10.3390/S25206317](https://doi.org/10.3390/S25206317).

- [11] K. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems," *Future Internet* 2024, Vol. 16, Page 339, vol. 16, no. 9, p. 339, Sep. 2024, doi: [10.3390/FI16090339](https://doi.org/10.3390/FI16090339).
- [12] A. F. Gentile, D. Macri, E. Greco, and P. Fazio, "IoT IP Overlay Network Security Performance Analysis with Open Source Infrastructure Deployment," *Journal of Cybersecurity and Privacy* 2024, Vol. 4, Pages 629-649, vol. 4, no. 3, pp. 629–649, Aug. 2024, doi: [10.3390/JCP4030030](https://doi.org/10.3390/JCP4030030).

The Relationship between Visual Style and Emotional Engagement in Mobile Tourism Applications

Stela Mincheva

Faculty of Fine Arts
VTU "St. St. Cyril and Methodium"
Veliko Turnovo, Bulgaria
stella.mincheva23@gmail.com

Veselka Stoyanova

Artillery, AD and CIS faculty
National Military University V. Levski
Shumen, Bulgaria
veselka_tr@abv.bg

Abstract— Mobile tourism applications are designed to deliver both functional usability and emotionally engaging experiences. This article examines how visual style is associated with emotional engagement in four mobile tourism applications used in Bulgaria: *100 Places Bulgaria*, *I Love Bulgaria*, *The Hundred National Tourist Sites of Bulgaria*, and *Opoznai.bg*. A comparative mixed-methods user experience design approach was employed, incorporating a seven-point *Likert scale* and an *Emo-card* assessment with 85 respondents, along with three task-based think-aloud interviews. The analysis concentrates on four recurring interface components: overall map appearance, menu layout, landmark distribution, and achievement screen design. The results indicate that a clearer visual hierarchy, well-structured content distribution, and more visible progress cues are linked to stronger positive emotional engagement. Among the cases analysed, *100 Places Bulgaria* exhibits the most positive emotional profile, whereas *Opoznai.bg* demonstrates functional strengths but weaker visual coherence. These findings support integrating affective measures into user experience evaluation for tourism-oriented mobile applications.

Keywords— mobile tourism applications, user experience, visual style, emotional engagement, interface design, tourism user experience.

INTRODUCTION

Mobile tourism applications serve as significant points of connection between users and destinations. In user experience (UX) research, experience encompasses not only efficiency and task completion but also perception, affect, and context of use [1], [2]. This perspective is particularly relevant in tourism, where digital products are expected to facilitate orientation and planning while also stimulating curiosity, pleasure, and motivation [3]. Thus, the present study aims to address the following research

question: In what ways is visual style related to emotional engagement in mobile tourism applications?

Visual style is more than decoration in interface design. Composition, hierarchy, consistency, contrast, and symbolic cues shape how users interpret and emotionally respond to digital environments [3], [5]. Emotional value and user engagement are central dimensions of interaction quality in digital products [6], [7].

In the Bulgarian design context, research on pictograms and visual communication is particularly relevant to mobile tourism applications. Pictograms, icons and simplified visual signs support faster recognition, reduce the need for lengthy textual explanation and help users orient themselves in visually dense information environments [8]. This perspective is especially applicable to tourism interfaces, where users often rely on maps, icons and symbolic cues before engaging with detailed textual content.

The visual communication systems developed for major international events also provide a useful perspective for the present research. Such systems demonstrate how identity, symbols, colour, pictograms and graphic consistency can create a recognizable communication environment across different cultures and languages [9]. In a similar way, mobile tourism applications depend on coherent visual identity and recognizable signs in order to guide users, communicate cultural content and stimulate emotional engagement.

The interaction-oriented aspect of the study can also be related to research on interactive visual works and the role of the observer-participant. Visual experience is not passive; it is formed through perception, action and participation [10]. This perspective is relevant to UX research because the user of a mobile tourism application is not only a viewer of visual content, but an active

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.176>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

participant who searches, selects, navigates, marks progress and responds emotionally to the interface.

Research on the design and creation of interactive visual works also supports the interpretation of mobile interfaces as dynamic visual environments rather than static graphic compositions [11]. Therefore, the present study treats map appearance, menu layout, landmark distribution and achievement screens as interactive visual components that influence both task support and emotional engagement.

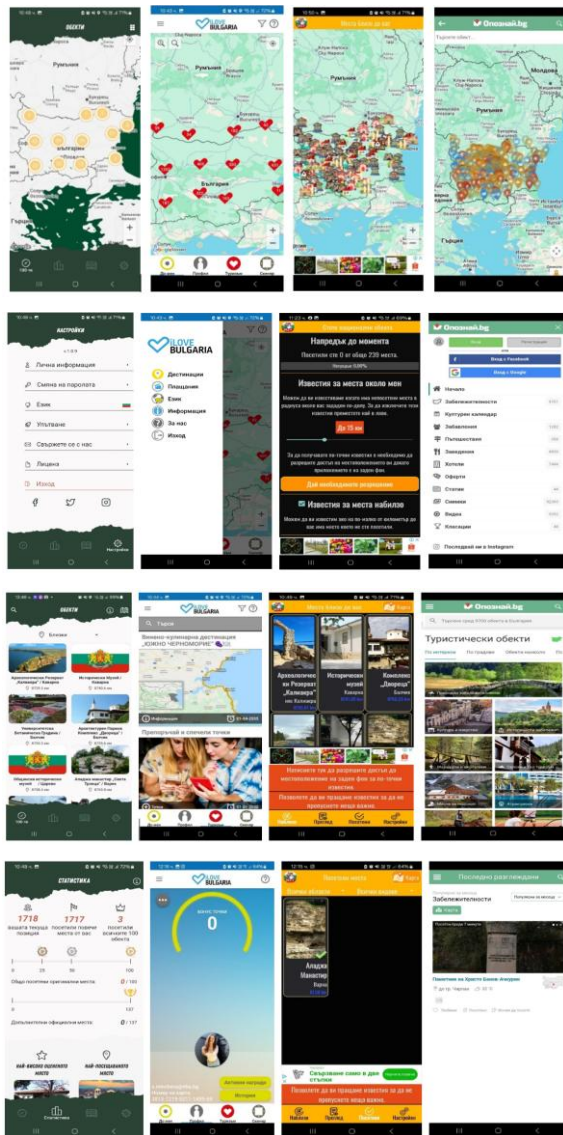


Fig. 1. Comparative interface examples of the four applications across the analysed components: map appearance, menu layout, landmark distribution, and achievement screen

This article examines a specific segment of the relationship between visual style and emotional engagement in four mobile tourism applications used in Bulgaria. Instead of conducting a comprehensive UX comparison, the analysis focuses on four recurring interface components identified through empirical

research: overall map appearance, menu layout, landmark distribution, and achievement screen design. The analysed applications and the four recurring interface components are illustrated in Fig.1.

This targeted approach enables a detailed examination of how particular visual characteristics are associated with more positive affective responses and stronger engagement.

• MATERIALS AND METHODS

The study uses a comparative mixed-method UX design, combining quantitative and qualitative approaches commonly used in UX evaluation [5], [12]-[15]. The analysis covers four Bulgarian domestic tourism applications: *I Love Bulgaria* [16], *The Hundred National Tourist Sites of Bulgaria* [17], *Opozna.bg* [18] and *100 Places Bulgaria* [19]. The comparison centres on four interface components found across all applications: map appearance, menu layout, landmark distribution, and achievement screen design. These components were selected because they combine navigational, visual, and motivational functions, making them suitable for examining the relationship between visual style and emotional engagement.

The quantitative phase involved 85 respondents: 52 women and 33 men, aged 21–62. Participants evaluated the applications using a seven-point Likert scale. The same group also used Emo-cards to assess affective responses along the dimensions *pleasant ↔ neutral ↔ unpleasant* and *interesting ↔ neutral ↔ boring*. The use of both tools enabled a comparison between reflective evaluation and a more immediate emotional response.

The qualitative phase included three individual think-aloud interviews: two men, aged 23 and 36, and one woman, aged 51. Participants completed tasks related to landmark discovery, route-related actions, and achievement functions. In the present article, these observations are used as a supporting interpretive layer for the visual-emotional findings rather than as a separate analytical focus.

The article adopts a comparative, descriptive-analytical logic, systematically contrasting each application across predefined interface components. This approach uses quantitative data, such as mean ratings for the four interface components and corresponding percentages of emotional responses, to identify patterns and differences across the applications. In addition, emotional positioning is assessed using the eight-category model to contextualise affective responses. The analysis is further supported by qualitative evidence from the think-aloud interviews, which provides insight into participants' experiences of visual order, navigation clarity, and the visibility of progress cues. By integrating these quantitative and qualitative data streams, the methodology enables a focused examination of how visual style is associated with emotional engagement. The sequence of the empirical procedure is summarized in Fig.2.

The selection of these components is also supported by visual communication theory, where pictograms, symbols and coherent graphic systems are understood as tools for orientation, recognition and cross-cultural readability [8], [9]. At the same time, the task-based part of the study reflects the idea that visual experience is shaped through active participation rather than passive observation [10].

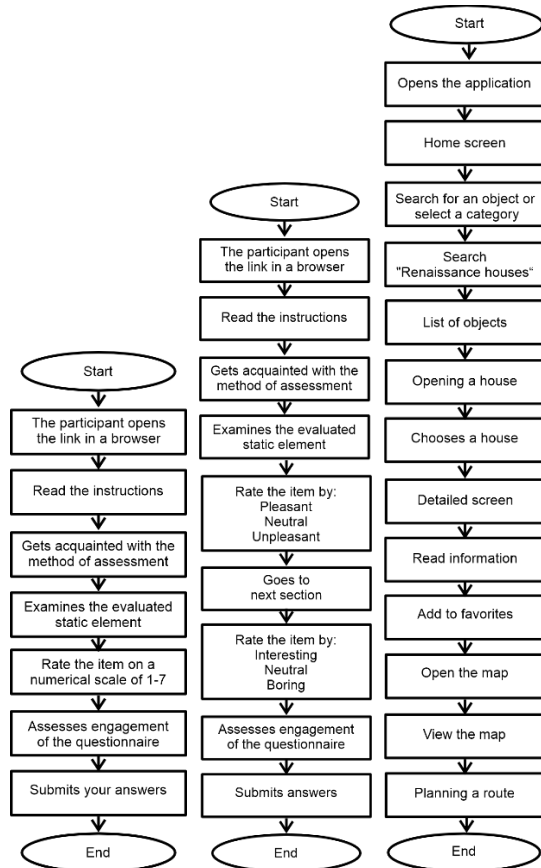


Fig. 2. Research design workflow showing the sequence of Likert evaluation, Emo-card assessment, and think-aloud interviews.

The affective dimension used in the Emo-card assessment are presented in Fig.3.



Fig. 3. Emo-card dimensions used in the study: pleasant–neutral–unpleasant and interesting–neutral–boring

RESULTS AND DISCUSSION

A. Quantitative Comparison of Interface Components

The comparative results (tabl 1.) show clear differences across the four applications. According to the empirical data, *100 Places Bulgaria* obtained the strongest combined profile, with mean scores of 4.92 for map appearance, 5.26 for menu layout, 5.89 for landmark distribution, and 5.52 for the achievement screen. *I Love Bulgaria* received 4.41, 4.98, 3.60, and 4.88, respectively. *The Hundred National Tourist Sites of Bulgaria* showed lower values across all four components, while *Opoznai.bg* displayed a mixed pattern, with a low score for map appearance but strong evaluations for menu layout and landmark distribution. Main values for the four compared interface components are presented in Table I.

TABLE I. MEAN VALUES OF THE COMPARED INTERFACE COMPONENTS

App	Criteria	Map	Menu	Landmark distribution	Achievement
100 Places Bulgaria		4.92	5.26	5.89	5.52
I Love Bulgaria		4.41	4.98	3.60	4.88
The Hundred National Tourist Sites of Bulgaria		3.54	3.98	4.06	4.34
Opoznai.bg		2.95	5.32	5.73	4.33

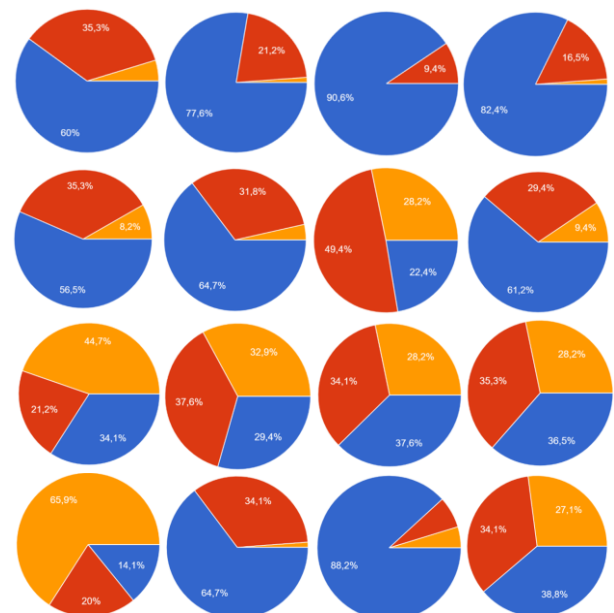


Fig. 4. Comparative emotional-response chart based on pleasantness and interestingness percentages for the four analysed interface components.

B. Emotional Assessment Through Emo-Cards

The emotional percentages further clarify the pattern. In *100 Places Bulgaria*, landmark distribution received ratings 90.6% pleasant and 87.1% interesting, while the achievement screen reached 82.4% pleasant and 76.5% interesting. In *I Love Bulgaria*, responses were more uneven, especially for landmark distribution, which received 22.4% pleasant and 23.5% interesting ratings. *The Hundred National Tourist Sites of Bulgaria* showed

consistently modest emotional ratings across the analysed components. In *Opoznai.bg*, landmark distribution was rated positively (88.2% pleasant and 85.9% interesting), but the map and achievement screen received substantially lower affective evaluations.

The comparative distribution of pleasantness and interestingness responses is visualized in Fig.4.

These data suggest that users' emotional responses are closely related to the interface's overall visual coherence. For example, *Opoznai.bg* achieved high positive ratings for landmark distribution, yet its lower scores for map appearance and achievement screens corresponded with weaker overall emotional engagement. This suggests that strong individual components do not fully compensate for weak hierarchy or visually overloaded composition.

C. Emotional Positioning of the Applications

The eight-category emotional model reveals a clear pattern. *100 Places Bulgaria* is positioned in the "Excited Pleasant" zone and is interpreted as engaging and inspiring. *I Love Bulgaria* is positioned in "Excited Neutral" indicating moderately positive engagement. *The Hundred National Tourist Sites of Bulgaria* is positioned in "Calm Neutral" suggesting balanced but weakly stimulating interaction. *Opoznai.bg* is associated mainly with "Excited Unpleasant" reflecting visual and informational overload. Emotional positioning of the four applications is shown in Fig.5.

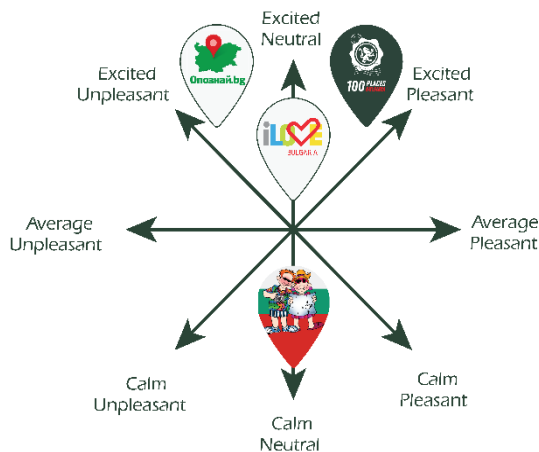


Fig. 5. Emotional positioning of the four applications within the eight-category emotional model

D. Supporting Observations From Task-Based Interviews

For the study was used the "Likert scale", according to which the user indicates a specific rating in an interval between two extremes – negative and positive, figure 6 shows the Rating scale for our study.



Fig. 6. Rating scale (1- I don't like it at all, 2- I don't like it, 3- I rather don't like it, 4- Neutral, 5- I rather like it, 6- I like it, 7- I really like it)

The criteria by which the audience evaluates dominants is how much they like them. The selected elements are the overall appearance, the web header, its main image and the main colour. Overall the sites are evaluated on how each one has chosen the combination of graphic elements and what is the impact on the target group [23].

The interview data support the quantitative and emotional findings. The map of *100 Places Bulgaria* was perceived as visually ordered, easy to scale, and logically structured. In *I Love Bulgaria*, route creation was rated as the easiest due to the automated logic that connects selected objects. *The Hundred National Tourist Sites of Bulgaria* was interpreted as functionally stable but visually limited. *Opoznai.bg* provided rich information, yet participants reported overload, poor visual focus, and difficulty locating functions. Only *100 Places Bulgaria* presented a clearly visible and emotionally rewarding achievement screen.

The main interview-based observation related to visual style, task support, and progress cues are summarized in Table II.

TABLE II. INTERVIEW-BASED OBSERVATIONS RELATED TO VISUAL STYLE AND TASK SUPPORT

Application	Visual style observation	Task support	Progress cues
100 Places Bulgaria	Clear, ordered, visually engaging	Easy landmark search and orientation	Easy to find, motivating
I Love Bulgaria	Visually appealing, moderately structured	Best route-creation support	Functional, less engaging
The Hundred National Tourist Sites of Bulgaria	Basic, restrained, outdated	Understandable but limited	Weak visibility
Opoznai.bg	Informationally rich but overloaded	Difficult to parse, weak focus	Low visibility and motivation

The interview observations confirm that the analysed applications function as systems of visual signs and interactive actions. Clear pictograms, recognizable symbols and consistent visual identity support orientation and reduce ambiguity, while weak hierarchy and overloaded screens interrupt the user's emotional involvement. This confirms the relevance of pictograms and visual identity to tourism interface design [8-9]. It also supports the view that aesthetic and user experience are formed through the active participation of the observer-user [10-11].

The results indicate a consistent association between visual style and emotional engagement. Applications with interfaces characterised by clearer hierarchy, better-organised spatial distribution, and visible progress cues

received more positive emotional evaluations. In particular, *100 Places Bulgaria* stood out because of the alignment between map design, landmark distribution, and achievement visualisation, resulting in the highest mean scores and the strongest positive emotional profile. These results suggest that visual clarity and progress visibility are important factors associated with stronger emotional engagement in mobile tourism applications.

Further analysis shows that strength in a single interface component does not guarantee a wholly positive emotional experience. Although *Opozna.bg* received high ratings for landmark distribution, its lower emotional scores for the map and achievement screen weakened the overall affective evaluation. This inconsistency suggests that when visually engaging elements are absent across the major components, the overall emotional response becomes less positive. Consequently, consistency and balance across interface components appear to be important for fostering stronger emotional engagement.

A further point concerns the role of progress visualisation. The interview data and component scores suggest that achievement screens should not be treated as secondary interface elements. When users can easily identify progress, unlocked elements, or visited places, the interface gains motivational value and supports emotional continuity over time [20]. This pattern is most visible in *100 Places Bulgaria* and least visible in *The Hundred National Tourist Sites of Bulgaria* and *Opozna.bg*.

Several design implications follow from these findings. First, map-based interfaces should prioritise visual simplification and a stronger layer hierarchy. Second, landmark distribution should support rapid visual parsing and orientation. Third, achievement screens should be treated as strategically important affective components rather than secondary pages. Fourth, visual consistency should be considered as important as functionality, since useful features lose effective value when embedded in visually noisy or fragmented environments.

The study also has limitations. Most importantly, the Emo-card method relies on respondents' subjective self-reports, which may lead to differences between experienced and reported emotional states. In addition, the three-level scale may oversimplify emotional responses. These limitations should be considered when interpreting the affective results. Despite this, the user-based recommendations in the broader study point in the same design direction: more filters and a more optimised map view for *100 Places Bulgaria*, improved search logic for *I Love Bulgaria*, a redesigned menu for *The Hundred National Tourist Sites of Bulgaria*, and visual simplification with stronger hierarchy for *Opozna.bg*.

CONCLUSIONS

This article examined one section of a broader study: the relationship between visual style and emotional engagement in four mobile tourism applications used in Bulgaria. The findings show that a positive emotional response is associated with visual clarity, a stronger hierarchy, a coherent distribution of landmarks, and clearly

visible progress cues. Among the analysed cases, *100 Places Bulgaria* demonstrated the strongest overall visual-emotional consistency, while *Opozna.bg* highlighted the limits of information-rich but visually overloaded design.

The study also indicates that affective evaluation should accompany usability-oriented assessment in tourism app research. Broader issues, such as user-flow analysis, route-creation logic, and wider usability comparison, can be developed as separate publications based on other sections of the same research.

FUTURE WORK

Future research may examine the role of artificial intelligence (AI) in the processing and interpretation of UX data. The framework proposed in [21] can serve as a practical instrument for organizations and development teams by supporting informed and sustainable decision-making regarding the integration of AI into web projects. In addition, the use of AI-based language models for generating aggregated reports from personalized interviews, as discussed in [22], may be relevant for future UX studies that combine qualitative interviews, structured templates, and automated report generation.

ACKNOWLEDGEMENT

The authors would like to thank that paper was supported by the National Scientific Program "Security and Defense", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022

The authors would like to thank that paper was supported by Faculty of fine arts, St Cyril and St Methodius University of Veliko Tarnovo.

The author would like to thank the participants in the empirical study and for the academic support provided during the development of the research on which this article is based.

I. REFERENCES

- [1] D. A. Norman, *The Design of Everyday Things*, rev. and expanded ed. New York, NY, USA: Basic Books, 2013, <https://dl.icdst.org/pdfs/files4/4bb8d08a9b309df7d86e62ec4056cef.pdf> [Accessed: March. 02, 2026].
- [2] E. L.-C. Law, V. Roto, A. P. Vermeeren, J. Kort, and M. Hassenzahl, "Towards a shared definition of user experience," in *Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI)*, Florence, Italy, 2008, pp. 2395–2398.
- [3] D. Buhalis and A. Amaranggana, "Smart tourism destinations: Enhancing tourism experience through personalisation of services," in *Information and Communication Technologies in Tourism 2015*, I. Tussyadiah and A. Inversini, Eds. Cham, Switzerland: Springer, 2015, pp. 377–389.
- [4] J. J. Garrett, *The Elements of User Experience: User-Centered Design for the Web and Beyond*, 2nd ed. Berkeley, CA, USA: New Riders, 2011.
- [5] A. P. Vermeeren, E. L.-C. Law, V. Roto, M. Obrist, J. Hoonhout, and K. Väänänen-Vainio-Mattila, "User experience evaluation methods: Current state and development needs," in *Proc. 6th Nordic Conf. Human-Computer Interaction (NordiCHI)*, Reykjavik, Iceland, 2010, pp. 521–530.

- [6] P. M. A. Desmet, C. J. Overbeeke, and S. J. E. T. Tax, "Designing products with added emotional value: Development and application of an approach for research through design," *The Design Journal*, vol. 4, no. 1, pp. 32–47, 2001.
- [7] H. L. O'Brien and E. G. Toms, "What is user engagement? A conceptual framework for defining user engagement with technology," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 59, no. 6, pp. 938–955, 2008.
- [8] Y. Yordanov, "Piktogramata kato sredstvo za vizualna komunikatsiya" ["The pictogram as a means of visual communication"], in *Proc. Int. Sci. Conf. Ot setivnoto kam vizualnoto – Pluralizmat v izkustvoto*, Veliko Tarnovo, Bulgaria, 2015, pp. 201–204.
- [9] Y. Yordanov, "Identichnost, traditsii i komunikatsiya na letnite olimpiyski igri" ["Identity, traditions and communication of the Summer Olympic Games"], in *Ot setivnoto kam vizualnoto – V tarsene na identichnostta*, Veliko Tarnovo, Bulgaria, 2019, pp. 180–187.
- [10] S. Kosev and A. Markov, "Vazpriyatie i deystvie v edno. Vazdeystvie na interaktivni art proizvedeniya varhu nablyudatelya-uchastnik" ["Perception and action in one. Impact of interactive art works on the observer-participant"], *Cultural and Historical Heritage: Preservation, Presentation, Digitalization*, vol. 6, no. 2, pp. 87–94, 2020, https://www.uni-vt.bg/userinfo/245/pub/17952/article_processes_a_markov.pdf [Accessed: March. 02, 2026].
- [11] S. Kosev and A. Markov, "Protsesi pri projektirane i izgrazhdane na interaktivni vizualni proizvedeniya" ["Processes for design and creation of interactive works in the visual arts"], in *Proc. Int. Sci. Conf. "Ot setivnoto kam vizualnoto – pluralizmat v izkustvoto"*, Veliko Tarnovo, Bulgaria, 2015, https://www.uni-vt.bg/userinfo/245/pub/17952/article_processes_a_markov.pdf [Accessed: March. 02, 2026].
- [12] D. A. Dillman, J. D. Smyth, and L. M. Christian, *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 4th ed. Hoboken, NJ, USA: Wiley, 2014.
- [13] J. Sauro and J. R. Lewis, *Quantifying the User Experience: Practical Statistics for User Research*, 2nd ed. Cambridge, MA, USA: Morgan Kaufmann, 2016.
- [14] E. Goodman, M. Kuniavsky, and A. Moed, *Observing the User Experience: A Practitioner's Guide to User Research*, 2nd ed. Waltham, MA, USA: Morgan Kaufmann, 2012.
- [15] J. Nielsen, "Thinking aloud: The #1 usability tool," Nielsen Norman Group, Fremont, CA, USA, 2012.
- [16] Website: ilovebulgaria.eu, Местен уеб сайт за пътувания <https://play.google.com/store/apps/details?id=net.loyalty&hl=en>, <https://ilovebulgaria.eu/> [Accessed: March. 02, 2026]
- [17] Website Стоте национални туристически обекта на България, Местен уеб сайт за пътувания, <https://play.google.com/store/apps/details?id=es.benesoft.turist&hl=bg> [Accessed: March. 02, 2026]
- [18] Website: [Opoznai.bg](https://opoznai.bg/), Местен уеб сайт за пътувания <https://play.google.com/store/apps/details?id=bg.opoznai&hl=bg>, <https://opoznai.bg/> [Accessed: March. 02, 2026].
- [19] Website 100те обекта, Местен уеб сайт за пътувания, https://play.google.com/store/apps/details?id=com.futurist_labs.bg_places&hl=en [Accessed: March. 02, 2026].
- [20] K. Werbach and D. Hunter, *For the Win: How Game Thinking Can Revolutionize Your Business*. Philadelphia, PA, USA: Wharton Digital Press, 2012.
- [21] S. Sulova, "Artificial Intelligence Tools in Web Application Development – Advantages and Challenges," 2025 International Conference on Intelligent Computing and Next Generation Networks (ICNGN), Singapore, Singapore, 2025, pp. 1-5, doi: 10.1109/ICNGN67480.2025.11413758 [Accessed: March. 02, 2026].
- [22] J. Vasilev, "The Use of MyGPT for Creating Aggregated Reports in Specific Report Templates Using Data From Personalised Interviews", *Information and Communication Technologies in Business and Education: Proceedings of the International Conference Dedicated to the 55th Anniversary of the Department of Informatics*, Varna, 2024, 42–46., ISBN (онлайн) 978-954-21-1184-9 [Online]. Available: https://informatics.ue-varna.bg/ICTBE2024/ICTBE2024_42-46.pdf [Accessed: April 01, 2026].
- [23] Mincheva, S., & Stoyanova, V. (2025). Research on the impact of the user experience for the success of a virtual product: Bulgarian travel agency websites. Resources: Proceedings of the 16th International Scientific and Practical Conference, 237–241. <https://doi.org/10.17770/etr2025vol2.8591>

AI Dependency in Higher Education: Are Students Becoming Over-Reliant?

Julija Mironova

Department of Management
Riga Nordic University
Riga, Latvia
julija.mironova@isma.lv

Viktorii Riashchenko

Department of Management
Riga Nordic University
Riga, Latvia
viktorii.riashchenko@isma.lv

Baiba Rivža

Department of Economics and Social
Development
LBTU
Jelgava, Latvia
rivzab@lbtu.lv

Valentina Djakona

Department of Management
Riga Nordic University
Riga, Latvia
valentina.djakona@isma.lv

Marina Celika

Department of Management
Riga Nordic University
Riga, Latvia
marina.celika@isma.lv

Ieva Nicgala

Riga Management College
Riga, Latvia
ieva.nicgala@college.lv

Abstract— Artificial intelligence has become part of daily life in universities, for both students and educators. However, despite the fact that we all understand that AI is shaping and changing the education paradigm, the question of how often and for what we use AI remains on the agenda. Yes, AI has made many daily tasks easier; however, are students using AI for tasks they could solve without it?

The aim of this study is to investigate the extent to which students in higher education are becoming dependent on artificial intelligence (AI) tools, particularly generative AI systems, in their academic activities. The study seeks to explore how frequent AI usage influences students' learning behaviors, critical thinking, and academic engagement.

This study employs a quantitative research design and a cross-sectional survey to examine students' dependence on AI tools in higher education. A structured questionnaire was developed to collect data on students' AI usage patterns, dependency levels, and perceptions of its impact on learning. The results of the study show the impact of AI on learning, academic integrity, self-perceived dependency, and risks, as well as how AI has changed the way students' study.

Keywords— Artificial intelligence, higher education, learning, academic integrity, risks, students.

I. INTRODUCTION

Currently, Artificial Intelligence technologies have become widely used in the context of higher education and transformed academic processes. Students now have more options for completing assignments, conducting research,

generating texts, engaging in discussions with virtual assistants and much more. However, these technologies present several opportunities and challenges - the application of AI has resulted in the appearance of new forms of educational products that enhance students' productivity, for example, students can easily generate texts, receive quick feedback from automated assistants, and find solutions to the problems they might face during the study process. Second, AI offers several benefits to students, such as saving time, receiving personalized assistance, and increasing the accessibility of learning resources. However, it is very clear that AI tools play an essential role in higher education today, as higher education has definitely changed with the launch of the AI generative tools a few years ago.

Nevertheless, despite the positive aspects associated with AI in higher education, certain concerns have arisen recently. Although students have multiple opportunities for learning with the help of artificial intelligence, there are worries that students might become too dependent on AI tools. Indeed, students can perform any task quickly without expending much effort by simply using AI. As a consequence, learners may no longer be engaged in independent thinking, analysis, and critical reflection. Besides, there is uncertainty in the scientific discussion about the influence of AI on students critical thinking and the way how they study.

Despite the vast literature related to the problems associated with the introduction of AI into education, information regarding the level of dependence on AI technologies by students and its consequences for their

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.174>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

learning process is extremely limited. While most of the literature focuses on the normative and ethical side of integrating artificial intelligence technologies in educational institutions, little research quantifies the use of these technologies by students. Furthermore, research is often deficient in analyzing the correlation between the variables mentioned above. To fill in these gaps, the purpose of this research is to identify the degree of students' dependence on AI tools in higher education. Furthermore, this study analyzes how students' AI usage frequency and their dependency on AI technologies affect their critical thinking, stress levels, and perceptions of academic integrity risks.

Theoretical Background and Hypothesis Development

1. The Dual Impact of Generative AI: Self-Efficacy and Technological Dependence

While the advantages of generative artificial intelligence (AI) are widely acknowledged, its increasing integration has instigated discussions regarding its implications for technological dependence and the cultivation of self-efficacy (Backfisch et al., 2021; Huang et al., 2024b). Self-efficacy, a foundational construct within educational psychology, denotes an individual's conviction in their capacity to successfully execute particular tasks, and it has been demonstrated to exert a substantial influence on learning motivation and academic achievement (Bandura, 1997). Technological dependence, conversely, refers to a pronounced reliance on specific digital tools and services, rendering them essential for daily operations and the accomplishment of objectives. Should this dependence reach a significant degree, the capacity to function effectively without the technology may be compromised (Davis, 1989)—a circumstance educational environments ought to proactively mitigate.

Empirical evidence indicates that generative AI can enhance student confidence and operational efficiency, consequently bolstering their self-efficacy (Liang et al., 2023b; Meyer et al., 2019; Yilmaz & Yilmaz, 2023). Conversely, extensive engagement with generative AI may cultivate undue technological dependence, which could potentially diminish students' capacity for autonomous problem-solving (Huang et al., 2020; Zhang et al., 2024). This inherent paradox presents a significant challenge: while immediate advantages, including improved learning efficiency and heightened confidence, are discernible, the protracted effects could potentially erode students' autonomous learning capabilities and psychological resilience.

Despite the existing literature underscoring the potential of generative AI to enhance learning outcomes, systematic inquiry into the dual impact of usage frequency on both self-efficacy and technological dependence remains limited (Huang et al., 2020; Zhang et al., 2024). A more comprehensive understanding of the intricate relationships among these variables represents a notable lacuna in current research. Accordingly, we propose the following hypothesis:

2. AI Dependence and Critical Thinking

Empirical investigations have consistently indicated that students exhibiting substantial reliance on AI tools tend to demonstrate diminished capacities in information evaluation and autonomous problem-solving (Bahrini et al., 2023; Hinss et al., 2022). This particular pattern of reliance has been attributed to cognitive inertia, a phenomenon where the recurrent outsourcing of cognitive processes results in a reduction of intellectual effort (de la Puente et al., 2024; Lee et al., 2025). Furthermore, instances of passive AI utilization, characterized by actions such as the uncritical reproduction of generated content, have similarly been associated with surface-level learning and a restricted comprehension of intricate subject matter (Dwivedi et al., 2023; Gerlich, 2025).

From a theoretical perspective, cognitive offloading provides a pertinent framework for understanding these observed effects. When students delegate specific cognitive tasks to AI systems, there is an observable reduction in their internal cognitive load; however, this often occurs at the potential expense of more profound cognitive processes, including inference, synthesis, and evaluation (Chaudhry et al., 2023; Storm et al., 2017). The habitual engagement in such offloading over an extended period has the potential to cultivate what has been termed "cognitive laziness," thereby impeding the development of higher-order thinking skills.

Nevertheless, the relationship between the utilization of AI and cognitive abilities is not exclusively detrimental. Certain investigations suggest that AI possesses the capacity to enhance critical thinking, particularly when integrated as a scaffold within active learning paradigms. For example, the strategic deployment of conversational AI, such as ChatGPT, to facilitate structured debates or to prompt the critical evaluation of its generated outputs, has been observed to foster heightened analytical reasoning and more profound engagement with subject matter (de la Puente et al., 2024; Supriyanti et al., 2020; Walter, 2024; Yilmaz & Yilmaz, 2023a). Consequently, the cognitive impact attributed to AI appears contingent upon the manner in which learners engage with these tools: when utilized in a reflective and appropriately regulated fashion, AI can indeed function as a catalyst for intellectual development; conversely, an approach characterized by excessive or passive reliance risks diminishing the very cognitive proficiencies it is intended to augment (Strzelecki, 2023). Drawing upon this rationale, we propose the following hypothesis:

3. AI Dependence and Academic Stress

Investigations into AI utilization have revealed that it presents a dual nature, offering both potential relief and additional burdens for users. While AI applications demonstrably enhance efficiency, students frequently express apprehension concerning the reliability and perceived fairness of the outputs generated by these systems (Chen et al., 2024). Moreover, Abbas et al. (2024) observed that a reliance on AI may compromise academic integrity and diminish student engagement, thereby introducing supplementary stressors pertaining to

self-doubt and external evaluative pressures. In a similar vein, Bermeo et al. (2024) reported that frequent reliance on AI tends to erode students' sense of agency, consequently exacerbating their evaluative stress.

Consistent with the transactional model of stress and appraisal (Lazarus & Folkman, 1984), these conditions are posited to intensify stress when an individual's perceived demands surpass their available coping resources. Importantly, AI dependence may amplify academic stress through multiple mechanisms—for instance, by reducing authentic social interaction or by undermining students' confidence in their own academic abilities. However, a detailed examination of these specific mediating pathways lies beyond the scope of the current study. Accordingly, we focus on the direct relationship and hypothesize:

4. Ethical Issues and Academic Integrity

The ethical challenges raised by AI are not minor or abstract. As Batista et al. (2024) and Perera & Lankathilaka (2023) observe, the distinction between assistance and deception becomes blurred when generative AI allows novel forms of academic dishonesty that evade detection. The creation of fake references—a documented weakness of certain GenAI systems—compounds the problem, eroding scholarly trust and muddying questions of attribution and originality (H. Wang et al., 2024). Kurtz et al. (2024) echo these worries, highlighting how GenAI-enabled cheating threatens educational integrity.

Beyond ethics, there is a more fundamental pedagogical concern: what does student learning look like when machines do too much? Cordero et al. (2025), D. Lee et al. (2024), and Zhang & Xu (2025) examine the danger of cognitive disengagement, arguing that learners may rely on GenAI to the point where they lose chances to practice creativity, reasoning, and problem solving. Batista et al. (2024) support this view, noting that without scaffolding, GenAI can end up bypassing deep engagement with course material altogether. However, in most of this critical literature, students' own views of GenAI—their interpretations, interest, confidence, or doubt—are seldom examined as influences on misuse. Given these points, we propose:

5. Regulatory Imperatives and AI Literacy

Despite the risks noted, there is agreement that AI's place in higher education is neither optional nor avoidable. As the literature keeps stressing, the path forward is not rejection but governance—grounded in institutional policies, ethical frameworks, and collective expectations (Batista et al., 2024; Cordero et al., 2025; Kurtz et al., 2024; D. Lee et al., 2024; Perera & Lankathilaka, 2023; H. Wang et al., 2024; Zhang & Xu, 2025). Nevertheless, any effective policy must reflect the diversity of higher education institutions and their learners. Yusuf et al. (2024) caution that cultural variability across global institutions renders one-size-fits-all policy frameworks unrealistic. Instead,

they argue for context-specific strategies sensitive to distinct educational values and ethical norms.

Central to this adaptation is GenAI literacy—not only for students but also for faculty and staff. Farrelly & Baker (2023) emphasize that responsible GenAI integration cannot be achieved without equipping educators with the tools to navigate it critically and creatively. They, together with McGrath et al. (2023), highlight frameworks such as those developed by Ng et al. and Hillier, which provide structured approaches to building GenAI literacy in academic environments. Zhang & Xu (2025) similarly underline that institutions must invest in upskilling their workforce, not merely to keep pace with technology but to shape its use in pedagogically sound and ethically aligned ways.

II. MATERIALS AND METHODS

For the purpose of this research, the authors developed a survey for the students of Higher Education. Survey was distributed during the period of time from February 2026 to April 2026. Survey was administered via Google Forms and all the data was collected anonymously. For the testing authors used Jamovi software.

The structure is presented in the Table 1.

TABLE 1 STRUCTURE OF THE SURVEY

Part	Structure of the survey	
	Question	Type of responses
A	Respondent profile	6 items: gender, age, level of study, field of study, year of study, region
B	Experience in usage of AI	7 items measuring frequency, duration, purposes of AI use, extent of academic reliance, and awareness/adherence to institutional AI policies (Likert scale, multiple choice, and percentage-based responses)
C	AI Reliance and Learning Impact	9 statements measuring students' reliance on AI, perceived effects on learning, critical thinking, and academic behavior (Likert scale: 1–5)
D	Student Stress and Psychological Support	3 items measuring perceived stress frequency, need for psychological support, and sources of academic pressure (Likert scale and multiple-response question)

To test the internal consistency of the part C, which later is used for AI Dependency Index, authors employed Cronbach's alpha in Jamovi. Block C (AI Reliance and Learning Impact) demonstrated high internal consistency, with a *Cronbach's alpha of 0.873*, suggesting that the items reliably measure a common underlying construct. Students from Europe and participated in the survey. Distribution of the respondents is presented in the Table 2.

TABLE 2 DISTRIBUTION OF THE RESPONDENTS BY REGION

Country	Counts	% of Total	Cumulative %
Europe	103	74.60%	74.60%
Asia	35	25.40%	100.00%

As can be seen from the findings, there is a great presence of the sample in Europe. In this regard, this aspect will affect the generalization of the findings. There is a smaller sample presence in Asia. Thus, the findings will be not compared from the perspective of the region in this study.

TABLE 3 DISTRIBUTION OF THE RESPONDENTS BY AGE

Age	Counts	% of Total	Cumulative %
More than 35	21	15.20%	15.20%
31-35	10	7.20%	22.50%
26-30	20	14.50%	37.00%
22-25	35	25.40%	62.30%
18-21	50	36.20%	98.60%
Under 18	2	1.40%	100.00%

The demographic structure suggests that the majority of the respondents are young students, specifically those between the ages of 18 to 25 years old. Therefore, the findings generated from this study reflect the views of the university students who are new to college life. The older age groups are less represented in this survey.

TABLE 4 DISTRIBUTION OF THE RESPONDENTS BY GENDER

Gender	Counts	% of Total	Cumulative %
Female	58	42.00%	42.00%
Male	78	56.50%	98.60%
Other	2	1.40%	100.00%

The ratio of gender is almost equal, but there are more males than females. However, there is no analysis in this specific articles based on the gender.

TABLE 5 DISTRIBUTION OF THE RESPONDENTS BY STUDY FIELD

Field of study	Counts	% of Total	Cumulative %
Other	19	13.80%	13.80%
Medicine	5	3.60%	17.40%

Manufacturing	1	0.70%	18.10%
Engineering	1	0.70%	18.80%
Mathematics	1	0.70%	19.60%
IT	35	25.40%	44.90%
Management	50	36.20%	81.20%
Finance	6	4.30%	85.50%
Economics	17	12.30%	97.80%
Education	3	2.20%	100.00%

From the data provided in the Table 5, it can be seen that the sample comprises more individuals in the field of management and IT than any other discipline.

TABLE 6 DISTRIBUTION OF THE RESPONDENTS BY STUDY LEVEL

Level of studies	Counts	% of Total	Cumulative %
Short cycle	8	5.80%	5.80%
Bachelors	82	59.40%	65.20%
Masters	37	26.80%	92.00%
PhD	11	8.00%	100.00%

The respondents who have registered for their bachelor's degree form the larger proportion of the sample size, hence the results can be applied to undergraduates.

TABLE 7 DISTRIBUTION OF THE RESPONDENTS BY STUDY YEAR

Study year	Counts	% of Total	Cumulative %
1	87	63.00%	63.00%
2	26	18.80%	81.90%
3	8	5.80%	87.70%
4	17	12.30%	100.00%

The sample contains a lot of first-year students, meaning that the results are primarily influenced by students who are still new to college life.

III. RESULTS AND DISCUSSION

For the analysis of the Block C, authors analysed students responses with the highest ranking – 4 and 5. Students were asked to rate statements from 1 to 5, where 1 is Strongly disagree, 5 is Strongly agree.

Table 8 shows the amount of the respondent who rated following statement with 4 and 5, and the % from the total share of the respondents.

TABLE 8 RESPONDENTS' AGREEMENT WITH STATEMENTS

Statement	Rated for 4 and 5	% from total share
-----------	-------------------	--------------------

I rely on AI to complete assignments	30	22%
I use AI even when I could solve tasks myself	25	18%
I feel uncomfortable studying without AI	29	21%
AI is my first option when facing academic challenges	29	21%
AI reduces my need to think deeply/critical thinking	38	28%
I trust AI answers without verifying them	21	15%
I rely on AI more than textbooks or course materials	26	19%
I feel more confident when using AI	31	22%
I feel stressed when I cannot use AI	14	10%

The results suggest a rather considerable level of usage of artificial intelligence (AI) among students, especially in situations associated with academic issues and efficiency.

The highest percentage agrees with the notion that "AI reduces my need to think deeply" - 28%, which means that almost 1/3 from the total share perceive AI as a means capable of replacing deep intellectual work. Therefore, this finding may raise concerns about critical thinking development among young people.

Also, it should be noted that a relatively high percentage of respondents

- I rely on AI to complete assignments -22%;
- I feel more confident when using AI - 22%; and
- AI is my first option when facing academic challenges - 21%.

Thus, these data prove that AI is not just an additional helper but an integral part of students' academic activity that contributes to their success and self-confidence.

On the one hand, 21% of participants find it uncomfortable to study without AI support, which may be a sign of forming some dependency on the technology. On the other hand, the signs of serious dependences among respondents are rather rare, namely

- only 10% of participants become stressed when AI is absent; and

- 15% of respondents trust all information received from AI without checking.

Overall, it means that while AI is actively used in students' work, its uncritical and emotional usage is quite common but not typical for most respondents.

Moreover, AI usage in academic work exceeds that of traditional sources such as textbooks or course materials in 19% of cases.

To reach the goal of the study, the following hypothesis is proposed:

H1: AI usage frequency is positively correlated with AI dependency;

H2: AI dependency is positively associated with reduced critical thinking;

H3: AI dependency is positively correlated with students' stress levels;

H4: AI dependency is associated with perceived academic integrity risks.

Firstly, authors created AI dependency Index, as there is no specific question "How/Are you dependent on AI", as the authors considered this question too direct and potentially leading to biased responses. Instead of that, following questions were included, and later AI dependency Index was created:

1. I rely on AI to complete assignments
2. I use AI even when I could solve tasks myself
3. I feel uncomfortable without AI
4. AI is my first option for academic challenges
5. AI reduces my need to think deeply/critical thinking
6. I trust AI answers without verifying them
7. I rely on AI more than textbooks
8. I feel more confident using AI
9. I feel stressed without AI

Average AI Dependency Index included above mentioned 9 statements. Based on the average scores ranging between 2.0 and 3.5 on a 5-point Likert scale, the level of AI dependency can be interpreted as moderate.

For the H1, authors employed Spearman's correlation test for 2 variables: AI Dependency Index and ranking of the students on how often do they use AI (1-never, 5-very often). The results revealed a statistically positive correlation between the two variables, $p = 0.001$; $\rho(138) = 0.272$. This indicates that students who use AI more frequently tend to exhibit slightly higher levels of dependency on AI tools. Therefore, H1 was supported.

For the H2, authors employed Spearman's correlation with the following variables: AI Dependency Index and ranking of the students about critical thinking. Results of the analysis revealed statistically moderate significant positive correlation with $p < 0.001$, $\rho(138) = 0.558$, indicating that higher levels of AI dependency are associated with greater perceived reduction in critical thinking. Therefore, H2 was supported.

For the H3, authors examined the relationship between AI Dependency Index and evaluation of the students on how often do they feel stress during their studies. Analysis showed that there is no significant relationship between AI Dependency Index and stress level of the students, what leads to the fact that H3 is not supported.

To test the last hypothesis – H4, authors used AI Dependency index and following statements, which are perceived academic integrity risks:

- AI tools can easily be misused in academic work
- Overuse of AI in studies can be considered dishonest
- It is difficult to distinguish between cheating and learning when using AI

The results indicated no statistically significant relationships between the variables, therefore, H4 is not supported.

As mentioned above, the current study provides new empirical evidence related to the growing prevalence of AI among college students and its potential connection with learning behaviors associated with dependence on external help. Based on the research findings, AI has become a part of the students' academic routine, though this influence varies across different dimensions.

First of all, H1 was confirmed as a statistically significant weak positive correlation between the frequency of using AI and the AI Dependency Index was obtained, $\rho(138) = 0.272$, $p = 0.001$. It means that the more often students use AI to complete their assignments, the higher is their AI dependency. Nonetheless, as indicated by the low strength of the relationship, the mere frequency of the AI use does not explain dependency issues fully. Namely, students can use the tool to support their activities or substitute it for completing academic assignments independently. In other words, dependency seems to be affected not only by the frequency but also by the mode and purpose of using the technology, along with a specific attitude toward it.

Secondly, H2 was also supported as a statistically significant moderate positive correlation between the variable of AI dependency and the perceived reduction in critical thinking was detected, $\rho(138) = 0.558$, $p < 0.001$. As noted above, this finding is quite interesting because it indicates that students, who are more dependent on AI, see this tool as a factor decreasing their critical thinking.

Hence, AI may be viewed as a facilitator of cognitive offloading, as a person may outsource intellectual activities to machines instead of analyzing situations, reflecting on them, and developing solutions independently. However, this result needs to be explained. The problem is that students themselves reduce critical thinking by using AI passively and not verifying the generated output and results critically.

Thirdly, H3 was not confirmed because a statistically significant relationship between AI dependency and the stress level was not found. This result might mean that there is no relationship between these variables. One of the reasons might be that the impact of AI on students' stress might be twofold, depending on how people use this technology. Namely, AI might reduce stress, for instance, by facilitating the completion of assignments and helping with understanding complicated topics. Meanwhile, using AI and being dependent on it may create additional uncertainty concerning academic misconduct and lead to anxiety. Therefore, researchers should distinguish between different kinds of stress in order to find the link between AI dependency and the emotional state of students.

Finally, H4 was not confirmed either as no statistically significant relationship between AI dependency and academic integrity risks was observed. As seen from this result, students do not always see their AI use as the violation of academic norms. Namely, they may consider this tool as one of the ways to facilitate learning activities and, hence, not as cheating. This is especially true as institutional policies in this area may be inconsistent, leading to confusion among students. Consequently, higher education institutions need to address this issue as they cannot assume that all students know where the boundaries lie regarding AI.

From the results presented above, it can be concluded that AI dependency in higher education is a rather complicated concept. The study does not argue that the technology itself is something negative. On the contrary, AI helps facilitate learning activities, increase access to information, and boost confidence. Nonetheless, the obtained findings demonstrate that this technology may affect the quality of learning processes negatively. In particular, the most interesting and alarming result of this study is the relationship between AI dependency and perceived reduction in critical thinking.

The obtained findings have certain practical implications. For instance, universities should develop specific guidelines on using AI in education. Namely, they need to explain students when and how to use this technology. In particular, students need to understand how to verify information generated using AI tools and what role such technologies play in the learning process in comparison with their actions. From this point of view, AI literacy

should become a necessary aspect of educational programs in higher education institutions.

In conclusion, the study had several limitations. First, the sample includes mostly students from Europe and first-year students. Secondly, the data were collected through surveys, so the results might be affected by respondents' subjective views. Finally, the cross-sectional nature of this study prevents the establishment of causal relationships. As a result, further research will require employing longitudinal designs, larger and more representative samples, and separate measurement of various variables discussed here.

REFERENCES

- [1] M. Abbas, F. A. Jam, and T. I. Khan, "Is it harmful or helpful? Examining the causes and consequences of generative AI usage among university students," *International Journal of Educational Technology in Higher Education*, vol. 21, no. 1, p. 10, 2024. doi: 10.1186/s41239-024-00456-3.
- [2] I. Backfisch, A. Lachner, K. Stürmer, and K. Scheiter, "Variability of teachers' technology integration in the classroom: A matter of utility!," *Computers & Education*, vol. 166, art. no. 104159, 2021. doi: 10.1016/j.compedu.2021.104159.
- [3] A. Bahrini, M. Khamoshifar, H. Abbasimehr, R. J. Riggs, M. Esmaili, R. M. Majdabadkohne, and M. Pashvar, "ChatGPT: Applications, opportunities, and threats," in *2023 Systems and Information Engineering Design Symposium (SIEDS)*, 2023, pp. 274–279. doi: 10.1109/SIEDS55613.2023.10132220.
- [4] A. Bandura, *Self-efficacy: The exercise of control*. New York: Freeman, 1997.
- [5] G. Barbayannis, M. Bandari, X. Zheng, H. Baquerizo, K. W. Pecor, and X. Ming, "Academic stress and mental well-being in college students: Correlations, affected groups, and COVID-19," *Frontiers in Psychology*, vol. 13, art. no. 886344, 2022. doi: 10.3389/fpsyg.2022.886344.
- [6] J. Batista, A. Mesquita, and G. Carnaz, "Generative AI and higher education: Trends, challenges, and future directions from a systematic literature review," *Information*, vol. 15, no. 11, p. 676, 2024. doi: 10.3390/info15110676.
- [7] S. D. R. Bermeo, M. L. Salazar, F. F. P. Terán, J. C. M. Calero, and V. J. A. Centeno, "Impact of AI on virtual learning: Self-sufficiency and academic confidence in university students," *Ciencia Latina Revista Científica Multidisciplinar*, vol. 8, no. 6, pp. 7414–7429, 2024. doi: 10.37811/cl_rcm.v8i6.15416.
- [8] J. T. Cacioppo and S. Cacioppo, "The growing problem of loneliness," *The Lancet*, vol. 391, no. 10119, p. 426, 2018. doi: 10.1016/S0140-6736(18)30142-9.
- [9] I. S. Chaudhry, S. A. M. Sarwary, G. A. El Refae, and H. Chabchoub, "Time to revisit existing student performance evaluation approaches in higher education in a new era of ChatGPT—A case study," *Cogent Education*, vol. 10, no. 1, art. no. 2210461, 2023. doi: 10.1080/2331186X.2023.2210461.
- [10] D. Chen, Y. Liu, Y. Guo, and Y. Zhang, "The revolution of generative artificial intelligence in psychology: The interweaving of behavior, consciousness, and ethics," *Acta Psychologica*, vol. 251, art. no. 104593, 2024. doi: 10.1016/j.actpsy.2024.104593.
- [11] J. Cordero, J. Torres-Zambrano, and A. Cordero-Castillo, "Integration of generative artificial intelligence in higher education: Best practices," *Education Sciences*, vol. 15, no. 1, p. 32, 2025. doi: 10.3390/educsci15010032.
- [12] F. D. Davis, "User acceptance of computer technology: A comparison of two theoretical models," *Management Science*, vol. 35, no. 8, pp. 982–1003, 1989. doi: 10.1287/mnsc.35.8.982.
- [13] M. de la Puente, J. Torres, A. L. Blanco Troncoso, Y. Y. Hernández Meza, and J. X. Márquez Carrascal, "Investigating the use of ChatGPT as a tool for enhancing critical thinking and argumentation skills in international relations debates among undergraduate students," *Smart Learning Environments*, vol. 11, p. 55, 2024. doi: 10.1186/s40561-024-00347-0.
- [14] Y. K. Dwivedi, N. Kshetri, D. L. Hughes, C. Coombs, J. S. Shareef, M. A. Shareef, and A. K. Kar, "So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy," *International Journal of Information Management*, vol. 71, art. no. 102642, 2023. doi: 10.1016/j.ijinfomgt.2023.102642.
- [15] A. Fanari and C. Segrin, "Longitudinal effects of US students' reentry shock on psychological health after returning home during the COVID-19 global pandemic," *International Journal of Intercultural Relations*, vol. 82, pp. 298–310, 2021. doi: 10.1016/j.ijintrel.2021.02.003.
- [16] T. Farrelly and N. Baker, "Generative artificial intelligence: Implications and considerations for higher education," *Education Sciences*, vol. 13, no. 11, p. 1109, 2023. doi: 10.3390/educsci13111109.
- [17] M. Gerlich, "AI tools in society: Impacts on cognitive offloading and the future of critical thinking," *Societies*, vol. 15, no. 1, art. no. 6, 2025. doi: 10.3390/soc15010006.
- [18] M. F. Hinss, A. M. Brock, and R. N. Roy, "Cognitive effects of prolonged continuous human-machine interaction: The case for mental state-based adaptive interfaces," *Frontiers in Neuroergonomics*, vol. 3, art. no. 898745, 2022. doi: 10.3389/fnrgo.2022.898745.
- [19] Y.-M. Huang, M. Y. Hsieh, and M. Usak, "A Multi-Criteria Study of Decision-Making Proficiency in Student's Employability for Multidisciplinary Curriculums," *Mathematics*, vol. 8, no. 6, art. 897, 2020. doi: 10.3390/math8060897.
- [20] S. Huang, X. Lai, L. Ke, Y. Li, H. Wang, X. Zhao, X. Dai, and Y. Wang, "AI technology panic—Is AI dependence bad for mental health? A cross-lagged panel model and the mediating roles of motivations for AI use among adolescents," *Psychology Research and Behavior Management*, vol. 17, pp. 1087–1102, 2024. doi: 10.2147/PRBM.S456789.
- [21] B. Klimova and M. Pikhart, "Exploring the effects of artificial intelligence on student and academic well-being in higher education: A mini-review," *Frontiers in Psychology*, vol. 16, art. no. 1498132, 2025. doi: 10.3389/fpsyg.2025.1498132.
- [22] G. Kurtz, M. Amzalag, N. Shaked, Y. Zaguri, D. Kohen-Vacs, E. Gal, G. Zailer, and E. Barak-Medina, "Strategies for integrating generative AI into higher education: Navigating challenges and leveraging opportunities," *Education Sciences*, vol. 14, no. 5, p. 503, 2024. doi: 10.3390/educsci14050503.
- [23] R. S. Lazarus and S. Folkman, *Stress, Appraisal, and Coping*. New York: Springer Publishing Company, 1984.
- [24] D. Lee, M. Arnold, A. Srivastava, K. Plastow, P. Strelan, F. Ploekl, D. Lekkas, and E. Palmer, "The impact of generative AI on higher education learning and teaching: A study of educators' perspectives," *Computers and Education: Artificial Intelligence*, vol. 6, art. no. 100221, 2024. doi: 10.1016/j.caeai.2024.100221.
- [25] H.-P. Lee, A. Sarkar, L. Tankelevitch, I. Drosos, S. Rintel, R. Banks, and N. Wilson, "The impact of generative AI on critical thinking: Self-reported reductions in cognitive effort and confidence effects from a survey of knowledge workers," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 2025, Paper no. 3713778, pp. 1–23. doi: 10.1145/3706598.3713778.
- [26] J. Liang, L. Wang, J. Luo, Y. Yan, and C. Fan, "The relationship between student interaction with generative artificial intelligence and learning achievement: Serial mediating roles of self-efficacy and cognitive engagement," *Frontiers in Psychology*, vol. 14, art. no. 1285392, 2023. doi: 10.3389/fpsyg.2023.1285392.
- [27] C. McGrath, T. C. Pargman, N. Juth, and P. J. Palmgren, "University teachers' perceptions of responsibility and artificial intelligence in higher education — An experimental philosophical study," *Computers and Education: Artificial Intelligence*, vol. 4, art. no. 100139, 2023. doi: 10.1016/j.caeai.2023.100139.

- [28] P. Perera and M. Lankathilaka, "AI in higher education: A literature review of ChatGPT and guidelines for responsible implementation," *International Journal of Research and Innovation in Social Science*, vol. 7, no. 6, pp. 306–314, 2023. doi: 10.47772/IJRIS.2023.70618.
- [29] D. Perlman and L. A. Peplau, "Theoretical approaches to loneliness," in *Loneliness: A Sourcebook of Current Theory, Research and Therapy*, L. A. Peplau and D. Perlman, Eds. New York: John Wiley & Sons, 1982, pp. 123–134.
- [30] B. C. Storm, S. M. Stone, and A. S. Benjamin, "Using the Internet to access information inflates future use of the Internet to access other information," *Memory*, vol. 25, no. 6, pp. 717–723, 2017. doi: 10.1080/09658211.2016.1210171.
- [31] A. Strzelecki, "To use or not to use ChatGPT in higher education? A study of students' acceptance and use of technology," *Interactive Learning Environments*, 2023, advance online publication. doi: 10.1080/10494820.2023.2209881.
- [32] S. Supriyanti, A. Permanasari, and F. Khoerunnisa, "Correlation between information literacy and critical thinking enhancement through PjBL-information literacy learning model," *Journal of Educational Sciences*, vol. 4, no. 4, pp. 774–784, 2020. doi: 10.31258/jes.4.4.p.774-784.
- [33] Y. Walter, "Embracing the future of artificial intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education," *International Journal of Educational Technology in Higher Education*, vol. 21, no. 1, p. 15, 2024. doi: 10.1186/s41239-024-00448-3.
- [34] H. Wang, A. Dang, Z. Wu, and S. Mac, "Generative AI in higher education: Seeing ChatGPT through universities' policies, resources, and guidelines," *Computers and Education: Artificial Intelligence*, vol. 7, pp. 2–11, 2024. doi: 10.1016/j.caeai.2024.100237.
- [35] Y. Wang and S. Xu, "Relationship between artificial intelligence tool usage experience and academic stress among college students: Mediating role of loneliness and moderating role of academic self-efficacy," *Acta Psychologica*, vol. 263, art. no. 106220, 2026. doi: 10.1016/j.actpsy.2025.106220.
- [36] R. Yilmaz and F. G. K. Yilmaz, "The effect of generative artificial intelligence (AI)-based tool use on students' computational thinking skills, programming self-efficacy and motivation," *Computers and Education: Artificial Intelligence*, vol. 4, art. no. 100147, 2023. doi: 10.1016/j.caeai.2023.100147.
- [37] R. Yilmaz and F. G. K. Yilmaz, "Augmented intelligence in programming learning: Examining student views on the use of ChatGPT for programming learning," *Computers in Human Behavior: Artificial Humans*, vol. 1, no. 2, art. no. 100005, 2023. doi: 10.1016/j.chbah.2023.100005.
- [38] A. Yusuf, N. Pervin, and M. Román-González, "Generative AI and the future of higher education: A threat to academic integrity or reformation? Evidence from multicultural perspectives," *International Journal of Educational Technology in Higher Education*, vol. 21, p. 21, 2024. doi: 10.1186/s41239-024-00454-5.
- [39] L. Zhang and J. Xu, "The paradox of self-efficacy and technological dependence: Unraveling generative AI's impact on university students' task completion," *The Internet and Higher Education*, vol. 65, art. no. 100978, 2025. doi: 10.1016/j.iheduc.2025.100978.
- [40] S. Zhang, X. Zhao, T. Zhou, and J. H. Kim, "Do you have AI dependency? The roles of academic self-efficacy, academic stress, and performance expectations on problematic AI usage behavior," *International Journal of Educational Technology in Higher Education*, vol. 21, no. 1, p. 34, 2024. doi: 10.1186/s41239-024-00467-0.

Generalized Net Model of the E-Learning Process

Daniela Mirtcheva-Ivanova
Bulgarian Defence Institute
"Professor Tsvetan Lazarov"
Sofia, Bulgaria
mirtchevadany@gmail.com

Rosen Iliev
Bulgarian Defence Institute
"Professor Tsvetan Lazarov"
Sofia, Bulgaria
r.iliev@di.mod.bg

Abstract: The paper presents a original model of the e-learning process, developed using the Generalized Net (GN) apparatus. The main stages in digital education are modeled - from access to learning resources in electronic platforms to ongoing control and final assessment. Through the GN-specific transitions, the logical connections and information flows between learners, teachers and learning management systems (LMS) are described. The model allows tracking individual progress and offers a theoretical basis for optimizing software architectures in the modern educational environment.

Keywords: e-learning, learning process, generalized net, education.

I. INTRODUCTION

The rapid development of information technology in the 21st century has led to an increase in the application of e-learning in education. In modern traditional education, lessons are built containing one, two or several electronic applications.

Many digital learning opportunities are offered. There are platforms with open online courses - these are generally available online courses with open access MOOC (Massive Open Online Course), which are offered by various universities and organizations around the world. Video sharing websites have been built, which provide a service to users for uploading, sharing, watching videos and live streaming. Content management systems (LCMS - learning content management system) are applied - computer software that provides the ability to create, store, manage and distribute content. Artificial intelligence (AI) is also an assistant in learning, which assists learners with instructions for solving tasks, tests and analyses in all academic disciplines and personalizes the learning process, analyzing the data of learners from the performance of tasks. Gamification, virtual and augmented reality in education (VR, AR) are used, simulations are applied, and many other existing and developing digital tools are increasingly present and entering education in the modern world [7].

II. MATERIALS AND METHODS

A model of the e-learning process was created, developed using the Generalized Networks (GN) apparatus and implemented using specialized software for creating generalized network models. The logical connections and information flows between students, teachers and learning management systems (LMS) were described using GN-specific transitions [1,2,4,6]

A flowchart of the e-learning process model was created using a graphical editor, logical connections and geometric figures, which implement the drawing of block structures [3].

The e-learning process model was tested using the GN IDE simulation environment to track the movement of the tokens and its operation. The simulation process was implemented using GN IDE (Generalized Nets Integrated Development Environment) and is an official software for simulating generalized network models [8, 9, 12, 13].

A model of teaching in the subject of informatics, including digital technologies, was applied.

The creation and testing of a new, more interesting and productive teaching method comes as a result of applied teaching in informatics with a variety of possible digital technologies with a group of students for a period of 4 months in a secondary school in Sofia in grade 12. A study was conducted between the results achieved in two groups of students after initial testing and proved almost the same result. The groups of 10 students were taught in different ways. One group used a programming environment and approved electronic textbooks for the subject. The other students used the same tools, as well as all possible digital technologies for the subject. As a result of the two different applied methods in teaching in informatics, the group using various digital technologies showed greater interest in learning, mastered the material faster and showed higher results. In the last testing in the study, the two groups showed a different result and a difference in achievements of about one unit.

A generalized network model of the e-learning process was created and proposed after research and review of

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.141>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

various materials in the field of generalized networks and learning [10, 11, 14, 15].

The e-learning process model structures the relationship between all participants through electronic platforms and contains:

1. Participants in the system:

- Teachers (mentors and designees) who set a lesson by creating learning content, setting tests and assignments and moderating the system;
- Students, learning part of the time independently, go through the learning content and provide feedback;
- Groups of students who work on projects, solve tasks and tests and teach each other.

2. Digital tools:

- Electronic platforms, such as LMS (Learning Management Systems), which store resources, conduct lectures, discussions, tests, and track student progress;
- Collaboration tools - Google Docs, Google Slides and tools for checking knowledge through gamification.

3. Model process. It takes place in the following stages:

Stage 1: Preparation of the platform and initial work of students

- The teacher prepares training materials and takes care of the design and moderates the system;
- Students work with the materials, including part of the time independently.

Stage 2: Collaborative work and analysis of student knowledge by the teacher

- Active learning through discussions of the material and tasks in Teams and Zoom in real time.
- Checking students' knowledge for an initial level of content by the teacher through surveys and tests prepared by him.

Stage 3: Student work in groups

- Groups of students work in a shared product and are present in a virtual classroom;
- The teacher monitors the work of the students and provides consultations.

Stage 4: Assessment and feedback

Groups share the results of the tasks through the screen of the digital device

- Through a test test in the electronic platform, the students' knowledge is assessed;

- The teacher monitors and analyzes the data from the group training to help with the students' difficulties
- A final assessment of the students' knowledge is made and a decision is made to move to the next module or study the material again.

Before creating a general network model of the e-learning process, we show the logic and connections between objects through a flowchart based on the stages through which learning occurs according to the presented model (Fig. 1) [3,5]

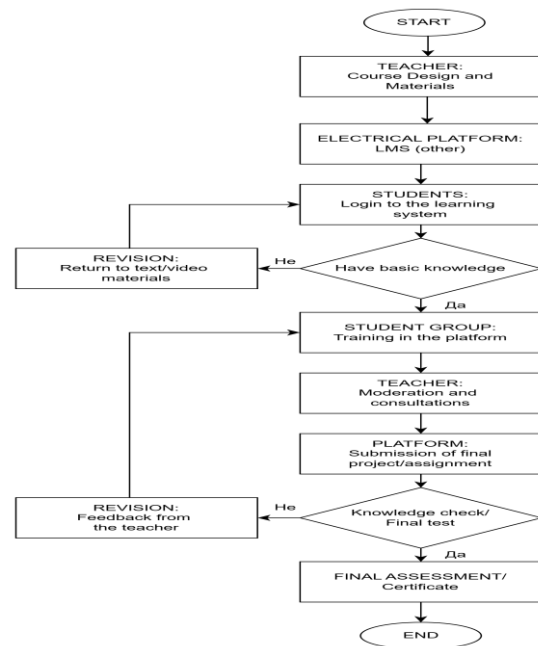


Fig. 1. Flowchart of an e-learning process model

Based on the description of the e-learning process model and as a continuation of the flowchart, its generalized network model was created [1,2,4,6] (Fig. 2).

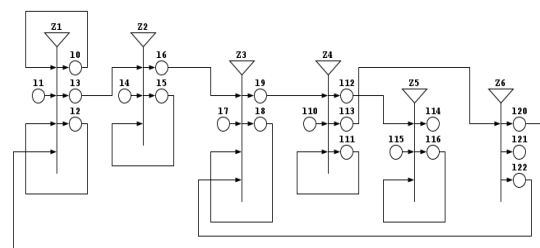


Fig. 2. Generalized net model of the e-learning process

The generalized network E contains the set of transitions $E = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$, where the transitions describe the following processes

The following tokens enter the OM network:

α – basic tokens and represent the students (learners)

- The tokens enter the model through position l_1 at the beginning of the scheme.

- The tokens accumulate in the review and feedback positions in the positions: l_2 – design; l_5 – materials; l_8 – test; l_{11} – task; l_{16} – certificate.

The tokens are split at position l_{13} of the transition Z_6 . The token is divided into logical copies at positions l_{21} – ends (discards), l_{22} – restart of the test, l_{20} – restart of the design.

- **The tokens merge** in the transition Z_1 – Here the tokens from the starting position l_1 and those returning for correction from l_{20} are merged in l_3 to start a new learning cycle (again).

- **The tokens merge** in the transition Z_3 – Here the tokens of the new students in position l_6 and those returning for correction of the test from l_{22} are collected in a common group for evaluation.

- **Token movement** - Tokens move in positions $l_1 \rightarrow l_3 \rightarrow l_5 \rightarrow l_9 \rightarrow l_{12} \rightarrow l_{14}$. Positions l_{20} and l_{22} are critical because they return the tokens to an earlier stage in the OM model to guarantee the quality of learning.

β – tokens – Tokens that enter positions $l_2, l_4, l_7, l_{10}, l_{15}$ carry resources. These are **information tokens** that carry materials and tests and merge with the main token of the student in the corresponding transitions.

γ – tokens – The tokens of the teachers – They create materials and play the role of controllers and evaluators in the OM model. They move in the feedback and control positions – l_0, l_{11}, l_{15} and l_{16} . The γ token enters through position l_0 and initiates the learning process. In l_{11} the teacher enters to help the students solve the task of learning the material and correcting errors. In positions l_{15} the teachers check and review the results of the training. In l_{16} administrative control is carried out when issuing documents.

In the model we have a conditional transition. The tokens receive the characteristics "test result", "certificate". If the result of any logical condition is false the token remains in position l_2, l_5, l_8 , or returns to the initial position l_1 through Z_6 , until the requirements for true are met.

Transition Z1: Preparation and design

Start of training

$$Z_1 = \langle \{l_1, l_2, l_{20}\}, \{l_3, l_2\}, r_1 \rangle$$

The tokens α enter through position l_1 or return from l_{20} for design correction.

The token γ enters through position l_0 and initializes the training process and remains in the system for creating materials, control and monitoring.

$$r_1 = \begin{bmatrix} & l_0 & l_3 & l_2 \\ l_0 & W_{0,0} & \text{False} & \text{False} \\ l_1 & \text{False} & W_{1,3} & W_{1,2} \\ l_2 & \text{False} & W_{1,3} & \text{true} \\ l_{20} & \text{False} & W_{1,3} & W_{1,3} \end{bmatrix}$$

$W_{1,3}$ = "There is a ready-made course design."

$W_{1,2}$ = "Additional training available"

Transition Z2: Training and materials

$$Z_2 = \langle \{l_3, l_4, l_5\}, \{l_6, l_5\}, r_2 \rangle$$

$$r_2 = \begin{bmatrix} & l_6 & l_5 \\ l_3 & W_{3,6} & W_{3,6} \\ l_4 & \text{false} & \text{true} \\ l_5 & W_{3,6} & \text{true} \end{bmatrix}$$

$W_{3,6}$ = "Have the learning materials been mastered"

Transition Z3: Testing and Evaluation

$$Z_3 = \langle \{l_6, l_7, l_8, l_{22}\}, \{l_9, l_8\}, r_3 \rangle$$

$$r_3 = \begin{bmatrix} & l_9 & l_8 \\ l_6 & W_{6,9} & W_{6,9} \\ l_7 & \text{false} & \text{true} \\ l_8 & W_{6,9} & \text{true} \\ l_{22} & W_{6,9} & W_{6,9} \end{bmatrix}$$

$W_{6,9}$ = "Entrance test passed"

Transition Z4: Solving a final assignment and feedback

$$Z_4 = \langle \{l_9, l_{10}, l_{11}\}, \{l_{12}, l_{13}, l_{11}\}, r_4 \rangle$$

$$r_4 = \begin{bmatrix} & l_{12} & l_{13} & l_{11} \\ l_9 & W_{9,12} & W_{9,13} & (W_{9,12} \ W_{9,13}) \\ l_{10} & \text{false} & \text{false} & \text{true} \\ l_{11} & W_{9,12} & W_{9,13} & \text{true} \end{bmatrix}$$

$W_{9,12}$ = "The task has been successfully solved"

$W_{9,13}$ = "Teacher assistance/correction needed"

Transition Z5: Certification

$$Z_5 = \langle \{l_{12}, l_{15}, l_{16}\}, \{l_{14}, l_{16}\}, r_5 \rangle$$

$$r_5 = \begin{bmatrix} l_{14} & l_{16} \\ l_{12} & W_{12,14} & W_{12,14} \\ l_{15} & \text{false} & \text{true} \\ l_{16} & W_{12,14} & \text{true} \end{bmatrix} 0$$

$W_{12,14}$ = "Certificate issued successfully"

Transition Z6: Feedback and restart

$$Z_6 = \langle \{l_{13}\}, \{l_{20}, l_{21}, l_{22}\}, r_6 \rangle$$

$$r_6 = \begin{bmatrix} l_{20} & l_{21} & l_{22} \\ l_{13} & W_{13,20} & W_{13,21} & W_{13,22} \end{bmatrix} 0$$

$W_{13,20}$ = "Return to design"

$W_{13,21}$ = "The student has exhausted the number of attempts or is giving up - the end"

$W_{13,22}$ = "Return to test"

Testing the model in the GN IDE simulation environment A simulation was performed on the general network model of the e-learning process to track the movement of the tokens and its operation. The simulation process was carried out using GN IDE (Generalized Nets Integrated Development Environment) and is an official software for simulation of generalized network models [8, 9]. Figures 3. and 4. show the movements of the α -tokens in the first transition of the e-learning process model, and Fig. 5. shows screens from the last stage of the movement of the tokens in the network. (Figure 3, Figure 4, Figure 5)

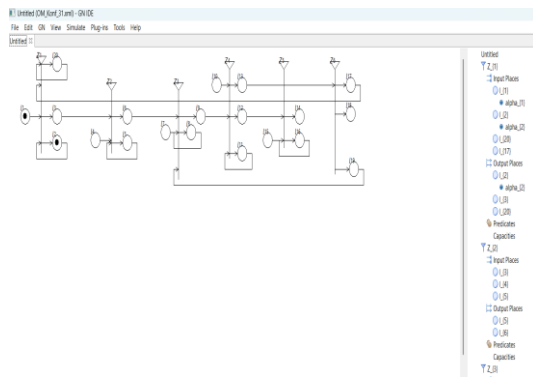


Fig. 3. Entry and movement of the α -token in the initial transition of the OM model.

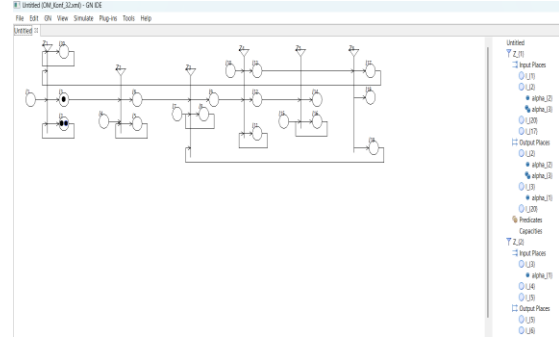


Fig. 4. Movement of the α -token in transition Z1.

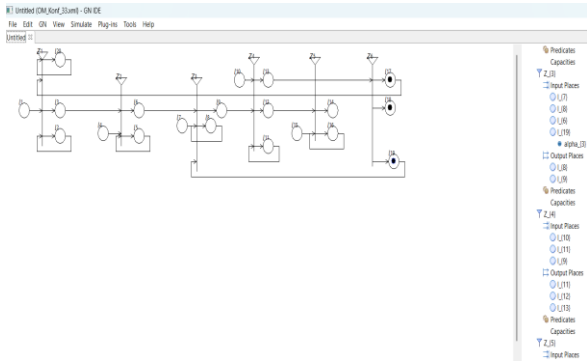


Fig. 5. Movement and realization of the α -token (learner) when using the e-learning process model

III. RESULTS AND DISCUSSION

The generalized net model of the e-learning process is up-to-date and effective. The training system monitors and automatically returns the student to a certain previous position without the intervention of the teacher (from positions l_{20} , l_{22}) for knowledge correction. The model offers personalization and tracking, by monitoring and deciding whether the student has the necessary knowledge for the next level through the predicates $W_{i,j}$. The OM model effectively manages resources through individual student and material tokens and allows updating of the learning content without interrupting the current learning of the students. The model tracks and analyzes the learning, progress and gaps (accumulation in l_8 and l_{11}) of the students thanks to the fact that each passage through a position leaves a characteristic.

IV. CONCLUSIONS

The OM model of the e-learning process is valuable with its tracking and personalization in learning, effective management of learning resources and feedback automation.

ACKNOWLEDGEMENTS

This work was supported by the National Science Program "Security and Defence" program, which has

received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

- [1] Atanassov, K., „Generalized Nets“, 1991
- [2] Atanassov, K. "On Generalized Nets Theory" (Published by "Prof. Marin Drinov", 2007)
- [3] Garvanov, I. "Modeling of Processes and Systems" (UniBIT, 2015)
- [4] Orozova, D., et al. "Generalized Net Model of E-learning System with Privacy and Security Requirements" (2009)
- [5] Sotirova, E., et al. "Generalized Net Model of a System for Quality Assurance in Higher Education" (2019)
<https://doi.org/10.1063/1.5133515>
- [6] Atanassov K. "Generalized Nets: Theory and Applications“, 2017. Available:
https://www.math.bas.bg/bgsiam/docs/bgsiam_2017_abstract-katanassov.pdf
- [7] Orozova D, Atanassov K., Todorova, M., January 2016 „Generalized net model of the process of personalization and usage of an e-learning environment“. Available:
https://www.researchgate.net/publication/311388385_Generalized_net_model_of_the_process_of_personalization_and_usage_of_an_e-learning_environment
- [8] Angelova N., M. Todorova, K. Atanassov, GN IDE: Implementation, Improvements and Algorithms, Comptes rendus de l'Academie bulgare des Sciences, Vol. 69, 2016, No. 4, 411—420, ISSN 1310-1331. https://www.proceedings.bas.bg/cgi-bin/mitko/0DOC_abs.pl?2016_4_02
- [9] Trifonov T., K. Georgiev, K. Atanassov. Software for modelling with Generalised Nets. Issues in intuitionistic fuzzy sets and generalized nets, Vol. 6, 2008, 36-42.10.
- [10] Boyukov T., Atanassov K., August 2025, Generalized nets as a tool for modelling of railway networks
https://www.researchgate.net/publication/394810745_Generalized_nets_as_a_tool_for_modelling_of_railway_networks_Part_3
- [11] Kochankov M., Iliev R., June 2024, A Generalized Net Model for Accessing Information Resources in a Secure Environment
https://www.researchgate.net/publication/399929712_a_generalized_net_model_for_accessing_information_resources_in_a_secure_environment
- [12] K. Atanassov K., 2020, Generalized Nets and Intuitionistic Fuzziness in Data Mining , Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences
- [13] Mathematical Objects Generated by an Arbitrary Natural Number - Krassimir Atanassov, Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences , 2024 г.
- [14] New Advances, Challenges, and Perspectives, National Conference on Operational and Systems Research, held in Warsaw, Poland on October, 17-18, 2024 Conference proceedings 2026, <https://doi.org/10.1007/978-3-032-22232-9>
<https://link.springer.com/book/10.1007/978-3-032-22232-9>
=Uncertainty and Imprecision in Decision Making and Decision Support -
- [15] Alexieva J., Sotirova E., May 2026, A Generalized Net Model for Implementation of Digital Competencies in the Education System, https://www.researchgate.net/publication/404678354_A_Generalized_Net_Model_for_Implementation_of_Digital_Competencies_in_the_Education_System

Intelligent Information System for Technical Supervision of High-Risk Facilities

Nikolay Nikolov

Faculty of Mechanical Engineering
Technical University of Sofia
Sofia, Bulgaria
nikolay.d.nikolov@tu-sofia.bg

Georgi Stanchev

Faculty of Mechanical Engineering
Technical University of Sofia
Sofia, Bulgaria
gstanchev@tu-sofia.bg

Boryana Ilieva - Mihaylova

Faculty of Mechanical Engineering
Technical University of Sofia
Sofia, Bulgaria
bilieva@tu-sofia.bg

Abstract—High-risk facilities (HRF) are subject to strict regulatory oversight, encompassing mandatory registration, periodic technical inspections, and systematic maintenance of technical documentation. In practice, the management of these processes is hindered by a range of organizational shortcomings: facility data are scattered across heterogeneous registers and files, there are no automated mechanisms for tracking inspection deadlines, and the document workflow between technical supervision bodies (TSB) and facility operators relies predominantly on paper-based and traditional communication channels. This paper presents the design and implementation of an intelligent information system (IIS) aimed at digitalizing and optimizing these processes. The applicable regulatory framework - the Law on Technical Requirements for Products and the relevant subordinate legislation and the identified practical challenges are examined. Based on interviews with representatives of TSBs and facility operators, system requirements were defined and a three-tier web architecture was proposed, implemented with React (presentation layer), Ruby on Rails (business logic), and PostgreSQL (data management), supplemented by Redis for session management and background job processing, and Active Storage for file handling. Access control is secured through JSON Web Tokens (JWT) and a role-based access control model (RBAC) with three levels - administrator, TSB and operator. The system centralizes the electronic technical record of each HRF, automatically calculates and monitors periodic inspection deadlines, generates mandatory documents and application forms, and provides a traceable document workflow with version control. Achieved results are presented alongside identified limitations - the absence of a mobile client, lack of integration with external national registries, and no support for qualified electronic signatures and directions for future development of the system are outlined.

Keywords— *high-risk facilities, technical supervision, information system, digitalization, document workflow, JWT, RBAC, Ruby on Rails, React, PostgreSQL.*

I. INTRODUCTION

High-risk facilities (HRF) are an integral part of modern industrial and public infrastructure. Boilers, pressure vessels, lifting cranes, gas equipment and installations, and others [3], [6], [7] – every type of them carries the potential for accidents and incidents.

The legal framework requires their registration, their safe and incident-free operation, and their compliance with the technical requirements, standards, and safety rules. In Bulgaria, this framework is set out by the Technical Requirements for Products Act (TRPA) [1] and the ordinances implementing it [2]–[5]. They introduce mandatory registration of the facilities and various technical inspections carried out by Technical Supervision Bodies (TSB) [4]. Each of these activities is accompanied by the drafting and submission of written applications, the preparation of inspection reports and protocols, and other documentation, the greater part of which continues to be kept and required on paper.

The data on each individual HRF is typically scattered across different people, files, and folders, with no one responsible for keeping it up to date as a whole. There is no mechanism to provide reminders of when a specific administratively defined deadline is approaching. Correspondence between TSBs and HRF operators is conducted through traditional channels, while the preparation of documents, reference notes, protocols, and reports is time-consuming and labour-intensive. Missed administrative deadlines are a systemic problem.

The present work proceeds from these findings and puts forward a concrete solution – an information system intended to replace existing practices with a unified digital environment for managing the technical file of an HRF, carrying out its technical supervision, and maintaining it in sound operating condition.

The aim is for the system to create and store an electronic technical file for each HRF, to track various

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.103>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

deadlines, to send notifications for approaching or overdue ones, to automatically generate the required applications, and to provide a shared working environment for TSBs, for HRF operators, and for the persons who maintain and repair them. The development was carried out within project No. 231ИП0035-06 and is structured in the following steps: analysis of the regulatory framework and existing practices; definition of the architecture; design of the logical model and the user interface; implementation and testing; evaluation of the results and outlining directions for further development.

II. DESIGN METHODOLOGY

The development follows a structured engineering approach [8], organised into eight sequential stages. The starting point is the pre-design study – an analysis of the current regulatory framework, observation of existing practices, and semi-structured interviews with representatives of TSBs and HRF operators. The aim of this stage is to define the problems and to verify whether the proposed solution is organisationally and technically feasible.

In the analytical phase, a formal logical model of the technical supervision processes has been built [9] – the main entities, their attributes, and the relationships between them have been identified. The model serves both as a specification for the developer and as a basis for validation with end users. The design is iterative: each functional core is followed by a short feedback cycle before moving on to the next. This approach allows for the early detection of discrepancies between regulatory requirements and technical implementation – a problem typical of regulation-bound systems.

The architectural decision was taken at the pre-design stage: a three-tier web architecture with a clear separation between the presentation layer, the business logic, and data management. The eight stages of the development are summarised in Table 1. The architecture of the system is shown in Figure 1.

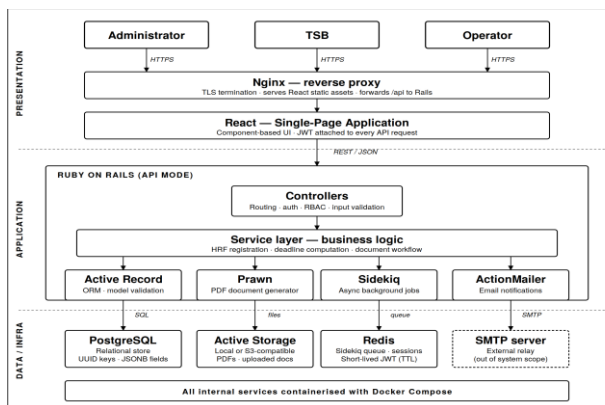


Fig. 1 Architecture of the information system

The client layer includes the three categories of system users: administrator, TSB, and HRF operator, each of whom interacts with the application through a web browser. Communication is encrypted, and every request passes through Nginx, configured as a reverse proxy.

Nginx performs a dual role: it serves the static files of the React application and forwards API requests to the server layer, thereby isolating the internal infrastructure from direct external access.

The server layer is implemented in Ruby on Rails in API mode and contains five logical modules. The controllers receive incoming requests, validate the data, and delegate the processing to the service layer. The business logic covers the rules for HRF registration, the calculation of deadlines, and document management. The automated tasks module (Sidekiq) operates asynchronously, periodically checking upcoming deadlines and triggering notifications without blocking the main application. The PDF generator (Prawn) produces the applications and lists required by the regulations. ActionMailer is responsible for sending email notifications to the TSBs that have registered a given HRF.

The data management layer is divided into three components with distinct purposes. PostgreSQL stores all structured data – the HRF registers, the technical file, the users, and the history of performed technical inspections, functional checks, and repairs. Active Storage manages the files associated with the technical files – inspection reports, protocols, instructions, declarations of conformity – and abstracts them from the specific storage medium, which allows a future transition to cloud storage without changes to the business logic. Redis is used for three separate purposes: storage of short-lived JWT tokens for password recovery, session management, and the queue of Sidekiq background jobs. The entire infrastructure is containerised with Docker Compose, which makes the configuration reproducible and simplifies the transition between test and production environments.

№	Stage	Outcome
1	Definition of scope and objectives	Scope description. Technical specification.
2	Study of the information system	Feasibility analysis. Key processes and entities.
3	Analysis of practices. Logical modelling	Formal logical model of the processes.
4	Planning. Conceptual design	General project description.
5	Detailed design	Structure. Functionalities. User interface.
6	Implementation	Development. Formal testing.
7	Deployment	System testing in a real environment.
8	Operation. Evaluation. Maintenance	Assessment of functioning and efficiency. Adjustments.

Table. 1 Stages of system design

III. DESCRIPTION OF THE INFORMATION SYSTEM

The information system is designed as a unified digital environment that brings together all processes related to the technical supervision of HRFs – registration of the facilities, management of documentation, tracking of deadlines for various types of technical inspections, and communication between the participants. The following

subsections describe, in turn, the architectural solutions, the logical data model, the mechanisms for authentication and access control, the management of documentation, and the module for automated notifications and document generation. Each of these components is designed to operate independently while also integrating seamlessly with the others – a principle embedded in the three-tier architecture of the system.

A. Architecture

The three-tier architecture [8] was chosen not as a formal convention, but as a practical response to the specific application context. In an environment where regulatory requirements change frequently, the ability to adapt only the business logic, without rewriting the interface or the database schema, is a real operational need rather than architectural overhead. A microservice decomposition [10], [11] was considered but rejected at this stage, as the operational complexity it would introduce is not justified by the scale of the domain.

The presentation layer is implemented as a Single Page Application with React [13]. The choice of the SPA model stems from the nature of the work with the data. System users deal with long forms, dynamic lists, and document previews, where a full page reload would significantly degrade usability. The React component model allows only the affected parts of the interface to be updated independently. Communication with the backend takes place entirely through a REST API, which makes the frontend technologically independent and, if necessary, replaceable without changes to the server-side logic.

The server layer is built with Ruby on Rails [12], configured in API mode, without the Rails templating mechanism, since the entire view is handled by React. Rails was chosen for its mature ecosystem for working with relational data, its built-in validation mechanisms, and its well-documented conventions for structuring business logic. Rails' Active Record allows the regulatory rules to be expressed directly as code – for example, the mandatory presence of a TSB for every registered HRF is enforced at the model level, not only on user input.

The database is PostgreSQL [14]. The choice over alternatives such as MySQL is determined by two specific requirements: support for UUIDs as primary keys without additional extensions, and JSON columns for storing the technical characteristics of the facilities, whose structure varies depending on the type of HRF. PostgreSQL supports indexing of JSON fields, which enables efficient filtering.

Redis [15] is used for three separate purposes: a queue for background jobs (Sidekiq), storage of password-recovery tokens with TTL, and session caching. Separating these three responsibilities into distinct Redis databases (by number) is deliberate and allows the cache to be flushed independently without the risk of deleting active jobs. Active Storage abstracts file storage: in the test environment, files are written locally, while the transition to cloud object storage requires a change only in the configuration, with no code modifications.

The entire stack is containerised with Docker Compose [16]. In the development environment, each service – Rails, the React dev server, PostgreSQL, Redis – runs in a separate container with defined dependencies. In the production environment, Nginx is added as a reverse proxy in front of the Rails application: it handles SSL termination, serves the static files of the React application directly from disk, and forwards only dynamic requests to the Rails process. This reduces the load on the Ruby process and allows the individual components to be scaled independently.

B. Logical model

The proposed model is built around the HRF as the central entity (HighRiskFacility), linked simultaneously to the TSB, the operator, and its technical documentation. The User can take on different roles depending on the organisational context. The model also includes standalone entities for notifications and reminders, since deadline management is a functional core of the system rather than a secondary add-on. Table 2 summarises the main entities and attributes of the model.

Entity	Main attributes	Description
User	id, email, role	System user
HighRiskFacility	id, reg_number, type, params	High-risk facility
Document	id, version, revision_date, file	Document from the technical file
Notification	id, type, status	Automated notification
Reminder	id, due_date, severity	Deadline reminder

Table. 2 Main entities in the system

C. Authorisation and access control

For identity authentication, the JSON Web Token (JWT) standard [17] is proposed. Upon successful login, the system is to issue a token with which all subsequent API requests are authenticated. Temporary password-recovery tokens are stored in Redis with a short validity period – an approach that does not require an additional database and is sufficiently secure for the intended use case.

Access rights are to be managed through a role-based access control model (RBAC) [18] with three roles: Administrator, TSB, and Operator. The distinction is not merely formal – TSBs register HRFs and add to their technical file, whereas operators can only access them for reading and attach their own documentation. The system also supports two-factor authentication with backup codes [20]. Table 3 shows the rights by role.

Functionality	Administrator	TSB	Operator
User management	Yes	No	No
Facility register	Yes	Yes	Own only
Adding and editing HRFs	Yes	Yes	No
Uploading documents	Yes	Yes	No

Viewing documents	Yes	Yes	Yes
Notifications and reminders	Yes	Yes	Yes
Generating reports and reference notes	Yes	Yes	Yes

Table. 3 Role model and main access rights

D. HRF and documentation management

The core of the proposed model is the electronic technical file of each HRF. When a new facility is entered, its registration and factory numbers, its kind, type, and technical characteristics and parameters are validated. The system must not allow the entry of data that is incompatible with the selected kind of facility or with the TSB exercising supervision over it. Documents are stored with support for versioning and revision dates; if an overwrite is attempted, a warning is displayed so that information is not lost by accident.

The system must automatically calculate the date of the next periodic inspection, including inspections involving different kinds of testing depending on the type of the facility and its date of manufacture. Inspection reports, protocols from functional checks, and other documents may be associated with each HRF.

E. Automated notifications and document generation

The notifications module is to operate on the basis of periodic background jobs that scan upcoming deadlines and prepare an email containing an application to the corresponding TSB, to be approved and sent by the HRF operator. The logic is deliberately simple, without complex infrastructure, since the events are predictable and calendar-determined.

For PDF document generation, the use of an appropriate library is envisaged – in the proposed implementation, Prawn. The system supports several types of reports, from lists of upcoming technical inspections to registers of lifting accessories, with the option of sorting by key attributes. The supported types are listed in Table 4.

Report type	Content	Format
Upcoming technical inspections	List and deadline	PDF
Overdue technical inspections	Status and dates	PDF
On-demand / extraordinary technical inspections	Statuses and deadline	PDF
Lifting accessories (LA)	Register (monthly)	PDF
All lifting equipment	Register (quarterly)	PDF
Written application for technical inspection	HRF and TSB data	PDF + email

Table. 4 Generated reports and documents

IV. FUNCTIONAL MODEL OF THE SYSTEM

The proposed functional model defines six main modules, whose interaction ensures full coverage of the processes involved in exercising technical supervision over HRFs. Each module is described through the requirements for its functionality, without being tied to a specific

implementation. The aim is to set out a clear specification that can serve as a basis for subsequent development and validation [19]. Table 5 summarises the modules and the requirements for each.

Module	Functional requirements
User management	Registration with verification, role profiles (Administrator / TSB / Operator), two-factor authentication, session management, and access recovery
HRF register	Creation, updating, and archiving of HRF records with validated technical characteristics; filtering by kind, TSB, operator, and operational status; automatic determination of deadlines for various types of technical inspections
Technical documentation	Electronic technical file for each HRF; inspection reports with revision date/year; overwrite control; role-based rights for uploading and viewing
Notifications and reminders	Automatic generation of notifications for approaching and overdue deadlines; delivery by email to TSBs; traceability of the status of each notification
Document workflow and reports	Automatic generation of written applications for technical inspections; PDF lists of lifting accessories and lifting equipment; sorting and filtering by key attributes; delivery by email
Administration	Management of users and facilities; system statistics and audit trail; protection against accidental deletion of critical records

Table. 5 Functional model - modules and requirements

A central principle of the model is the separation of responsibilities: TSBs register and maintain the information on HRFs. Operators have access only to their own facilities and may only attach documents such as protocols from functional checks. The administrator manages the system but does not replace the role of the TSB. This distinction is dictated not by technical convenience, but by the logic of the TRPA and the various ordinances. The system must reflect actual powers, not blur them.

The notifications module is a functional core of the system, since it addresses directly the main problem identified – missed administratively defined deadlines. The requirement is that notifications be generated automatically, without any action on the part of the user, and reach the TSB and the operator simultaneously. In this way, the responsibility for tracking deadlines is not imposed on one side alone, but is shared and transparent.

The model is technologically neutral. The requirements described can be implemented using different technology stacks. A subsequent work will present a concrete implementation based on the proposed model, including a description of the chosen technologies, the testing results, and an assessment of the system's fitness for use in a real environment.

V. COMPARISON WITH GENERAL-PURPOSE SCHEDULING SYSTEMS

A reasonable question is whether widely used general-purpose scheduling tools, such as Microsoft Outlook or Google Calendar, could replace the proposed system.

These tools are mature and overlap with part of the functionality described above: they support deadline reminders, recurring events, shared visibility, and basic collaboration. For an organisation that tracks only a small number of inspection dates, a shared calendar may even be sufficient.

The difference lies in scope. General scheduling systems treat every entry as a generic, unstructured event and have no model of the regulated domain. The proposed system, by contrast, is organised around the HRF as a typed entity, together with the obligations attached to it. A calendar entry can remind a user that an inspection is due, but it cannot derive that date from the applicable ordinance, link it to the technical file of the facility, enforce which role may act on it, generate the required statutory application, or retain a traceable record of what was done and when. Table 6 summarises this functional difference.

Capability	Outlook / Google Calendar	Proposed system
Reminders, recurrence, shared visibility	Yes	Yes
Structured HRF records (typed entities, technical attributes, history)	No	Yes
Automatic regulatory deadline calculation from rule sets	No	Yes
Document versioning and revision control	No	Yes
Role-specific workflows (TSB / operator / administrator)	Limited / manual	Yes
Automated generation of applications and PDF documents	No	Yes
Audit trail and compliance traceability	No	Yes

Table. 6 Comparison with general-purpose scheduling systems

In short, a general scheduler answers only the question of when, whereas regulatory technical supervision additionally requires what, who, under which rule, and with what evidence – none of which such tools provide on their own. This is precisely what motivates a domain-specific compliance-management system rather than the adaptation of a general scheduling tool.

VI. CONCLUSION

The proposed model is built around the provisions of the applicable regulatory acts, not against them. Particularly important is the principle of automated notification. The problem of missed deadlines is systemic and cannot be solved through organisational measures alone without a supporting technological infrastructure. The role-based distinction between TSBs and operators reflects the actual powers under the TRPA and its implementing ordinances, while the technological neutrality of the specification allows implementation on different stacks depending on the organisational context.

Three areas have been deliberately left for the next phase of development: mobile access with offline mode and synchronisation, integration with public registers, and support for a qualified electronic signature (QES). Including them in the main scope would complicate the model to the point where its validation in a real environment would be difficult. The stepwise approach – first a model, then an implementation, then an extension – is justified by the complexity of the subject area. In the longer term, the accumulated history lays a foundation for predictive models that optimise the schedules of the stakeholders.

The present paper proposes a functional model of an information system for the technical supervision of HRFs, built on an analysis of the applicable regulatory framework and of the practical problems established in the sector. The model defines six functional modules, the principles of role-based access differentiation, and the architectural framework within which they are to interact. The main contribution lies not in the technological implementation, but in the systematisation of the requirements – a step which, in systems of this kind, is often omitted or carried out implicitly.

The three functional priorities of the model – a centralised electronic file, automated deadline tracking, and the generation of regulatorily required documents and applications – have been determined on the basis of a study conducted with representatives of TSBs and HRF operators. It is precisely at these three points that existing practices are labour-intensive, unsustainable, and difficult to trace. The model does not claim to solve all problems in the sector, but rather to have begun solving the problems identified.

The architectural framework proposed in the paper is three-tier and technology-independent. Beyond being good practice, the separation between the presentation layer, the business logic, and data management is a precondition for resilience in a strict regulatory environment subject to constant change. A concrete implementation based on the proposed model – including the choice of technologies, a detailed description of the implementation, and results from testing in a real environment – is the subject of a subsequent publication.

The defined limitations of the model – mobile access with offline mode, integration with external registers, and QES support – are not omissions but deliberately deferred requirements. Their inclusion in the main scope would complicate the model to the point where its validation in a real environment would be impeded.

In a broader context, the proposed approach – systematisation of regulatory requirements, definition of a functional model, and subsequent implementation – is applicable in adjacent regulatory areas as well [21]–[23]: fire safety, construction supervision, and licensing regimes – which is also the starting point of the present work. The authors regard this paper as the first in a series aimed at systematically addressing these problems.

REFERENCES

- [1] Law on the Technical Requirements for Products (ZTIP), State Gazette of the Republic of Bulgaria, no. 86/1999, last amended SG no. 21/2021. (in Bulgarian)
- [2] Law on Health and Safety at Work (ZBUT), State Gazette of the Republic of Bulgaria, no. 124/1997, last amended SG no. 9/2023. (in Bulgarian)
- [3] Ordinance on the safe operation and technical supervision of lifting equipment (NBETNPS), State Gazette of the Republic of Bulgaria, no. 78/2004. (in Bulgarian)
- [4] Ordinance on the conditions and procedure for issuing licences for technical supervision of high-risk facilities and for maintaining a register of the facilities (NURILOTNSPORVRS), State Gazette of the Republic of Bulgaria, no. 79/2003. (in Bulgarian)
- [5] Ordinance No. 1 of 2002 on the conditions and procedure for acquiring and recognising qualifications for practising professions in the operation of lifting cranes and mobile work platforms, State Gazette of the Republic of Bulgaria, no. 51/2002. (in Bulgarian)
- [6] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery, Official Journal of the European Union, L 165, 29 June 2023.
- [7] Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment, Official Journal of the European Union, L 189, 27 June 2014.
- [8] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*, 3rd ed. Upper Saddle River, NJ: Addison-Wesley Professional, 2012.
- [9] M. Fowler, *Patterns of Enterprise Application Architecture*. Boston, MA: Addison-Wesley, 2002.
- [10] C. Richardson, *Microservices Patterns: With Examples in Java*. Shelter Island, NY: Manning Publications, 2018.
- [11] S. Newman, *Building Microservices: Designing Fine-Grained Systems*, 2nd ed. Sebastopol, CA: O'Reilly Media, 2021.
- [12] D. H. Hansson, "Ruby on Rails: The Guide," Rails Core Team, 2024. [Online]. Available: <https://guides.rubyonrails.org>. [Accessed: Mar. 2025].
- [13] Meta Open Source, "React — A JavaScript library for building user interfaces," 2023. [Online]. Available: <https://react.dev>. [Accessed: Mar. 2025].
- [14] PostgreSQL Global Development Group, "PostgreSQL 16 Documentation," 2023. [Online]. Available: <https://www.postgresql.org/docs/16/>. [Accessed: Mar. 2025].
- [15] Redis Ltd., "Redis Documentation," 2023. [Online]. Available: <https://redis.io/docs>. [Accessed: Mar. 2025].
- [16] Docker Inc., "Docker Compose Documentation," 2023. [Online]. Available: <https://docs.docker.com/compose/>. [Accessed: Mar. 2025].
- [17] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," Internet Engineering Task Force (IETF), RFC 7519, May 2015. doi: <https://doi.org/10.17487/RFC7519>
- [18] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, 2nd ed. Norwood, MA: Artech House, 2007.
- [19] Systems and software engineering — Systems and software quality requirements and evaluation (SQuARE) — System and software quality models, ISO/IEC Standard 25010:2011, 2011.
- [20] Information security, cybersecurity and privacy protection — Information security management systems, ISO/IEC Standard 27001:2022, 2022.
- [21] M. Janssen and N. Helbig, "Innovating and changing the policy-cycle: Policy-makers be prepared!," *Government Information Quarterly*, vol. 35, no. 4, pp. S99–S105, 2018. doi: <https://doi.org/10.1016/j.giq.2015.11.009>
- [22] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, no. 4, p. 101385, 2019. doi: <https://doi.org/10.1016/j.giq.2019.06.002>
- [23] I. Lindgren, C. Ø. Madsen, S. Hofmann, and U. Melin, "Close encounters of the digital kind: A research agenda for the digitalization of public services," *Government Information Quarterly*, vol. 36, no. 3, pp. 427–436, 2019. doi: <https://doi.org/10.1016/j.giq.2019.03.002>

Why Did Threat Actors Replace PoshC2 with SliverC2? Comparison of Two Great C2 Frameworks

Dimitar Nikolov

IT Department

Nikola Vaptsarov Naval Academy

Varna, Bulgaria

d.nikolov@naval-acad.bg

Abstract – This paper presents a comparative analysis of the command-and-control (C2) frameworks PoshC2 and SliverC2, examined within the context of evolving adversarial tradecraft, shifting infrastructure paradigms and the increasing maturity of defensive capabilities. While C2 frameworks are traditionally associated with the post-exploitation phase, this study adopts a broader perspective, arguing that framework selection reflects not only tactical requirements but also strategic and operational adaptations to a rapidly changing cyber environment. The analysis is based on the recent transformations in enterprise infrastructure, notably the transition from predominantly on-premises, Active Directory-centric Windows environments to complex, distributed, and hybrid cloud ecosystems. This evolution, combined with the expanded attack surfaces across critical sectors, has imposed new constraints on adversary operations. In parallel, defensive practices have become increasingly proactive and intelligence-driven, with widespread adoption of EDR, XDR and SIEM solutions. These developments have contributed to a significant reduction in attacker dwell time and increased detection of well-established tools, techniques, and procedures (TTPs). Within this context, the paper contrasts the architectural and operational characteristics of PoshC2 and SliverC2. PoshC2 is a mature, PowerShell-centric framework optimized for Windows environments, offering extensive post-exploitation functionality but exhibiting increased detectability due to its reliance on heavily monitored technologies. In contrast, SliverC2 represents a modern, Golang-based, cross-platform approach, emphasizing dynamic payload generation, modular extensibility, and advanced communication protocols. The findings of this paper indicate that the shift from PoshC2 to SliverC2 reflects adaptive adversary behavior driven by environmental complexity and defensive pressure, rather than a simple tool substitution. Contemporary offensive operations are inherently multi-framework, with tooling selected dynamically based on operational requirements and target characteristics.

Keywords – *Adversarial tradecraft, command-and-control frameworks, cyber operations, infrastructure paradigms, post-exploitation.*

I. INTRODUCTION

When talking about command and control (C2) frameworks they are often viewed in the context of post exploitation. While that is correct from attacker's tactical point of view, since C2 frameworks are used primarily at this stage, in order to fully understand why hackers shifted from using PoshC2 to SliverC2, things like strategic priorities shifts, as well as attackers and defenders changes in tradecraft and TTP's should be taken in consideration. This article intends to analyze the approaches and capabilities offered by both frameworks and makes a comparison of the advantages and disadvantages they have.

Some of the major changes that happened to infrastructure in the recent years is the shift from totally on premises, mainly Active Directory based, Windows environments to a highly technologically and geographically diversified cloud based and hybrid environments. Complexity of the infrastructure has also dramatically increased. Mobile devices, BYOD, laptops and tablets are much more common including in critical infrastructure environments, in the energy, financial and transportation sectors. APT's like Salt Typhoon have been specifically targeting telecommunication companies, in essence positioning themselves for service supply chain attacks against critical infrastructure.

On the other hand, defensive tradecraft has evolved and is currently much more threat hunt and cyber threat intelligence oriented and driven. PowerShell, WMI, CIM and commonly used by C2 network protocols like HTTP, HTTPS, DNS and SMB use are heavily monitored. This combines with the enhanced use of EDR, XDR and SIEM by the SOC teams, creating dynamic and highly

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.212>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

environment for the hackers. Dwell times in the recent years have gone down from over 300 days to 10 leaving much shorter window of opportunity for the adversary.

II. POSHC2

PoshC2 was developed by Nettitude (now LRQA) and first released in July 2016 [1]. It is a multi-user, proxy-aware, command-line C2 framework focused on Windows exploitation and post-exploitation, with PowerShell, C#, and Python capabilities. The server is written in Python 3, agents are PowerShell- and C#-based. Version 8 introduced a Linux agent and Beacon Object File (BOF) execution via Joel Snape's RunOF in 2022. In-memory execution of PowerShell and C#/ .NET assemblies is provided through a module system invoked by .NET reflection, though this requires additional configuration. Designed for quiet operation using fileless, in-memory implants and encrypted HTTP/S communication, PoshC2 ships pre-configured modules for Mimikatz, keylogging, lateral movement via WMI/PsExec, and automated Active Directory enumeration.

These capabilities, together with out-of-the-box download cradles and shellcode of multiple variants, made PoshC2 attractive to operators when it appeared, and it became a popular choice alongside other heavy PowerShell users such as Empire. Over the following years, however, Microsoft systematically eroded the advantages that PowerShell-centric tooling depended on, introducing in particular:

- 1) System-wide transcription - a Group Policy-enabled auditing mechanism, introduced in Windows PowerShell 5, that records commands, script blocks, and output to text files for every user on a host.

- 2) Script-block logging - a runtime mechanism that captures the full content of PowerShell script blocks as they are processed by the engine, yielding far richer records than command-line logging.

- 3) The Antimalware Scan Interface (AMSI) - introduced in 2015, which gives antimalware products visibility into the PowerShell engine, script hosts (wscript.exe, cscript.exe), Office macros, the .NET Framework, and WMI components frequently abused in living-off-the-land and fileless techniques [3].

- 4) Constrained Language Mode (CLM) - which restricts advanced PowerShell features-custom .NET methods, COM objects, and Windows API calls-typically enforced through AppLocker or Windows Defender Application Control (WDAC) [4].

Individually, each of these controls is bypassable, taken together they make the Windows environment markedly more hostile to PowerShell abuse. The pre-built download cradles, shellcode, and droppers that were once a PoshC2 advantage became largely impractical without heavy customisation and obfuscation. This shift-combined with the large number of public signatures for PoshC2 implants, intensive PowerShell monitoring and restriction, improved antimalware engines such as Microsoft Defender, and routine hunting for WMI/PsExec lateral-movement indicators-created pressure for a different approach.

Operators moved toward flexible in-process use of assemblies and avoidance of fork-and-run execution (an approach popularised by Cobalt Strike's BOFs), and toward implants able to run on Linux, Unix, and macOS as well as in cloud and hybrid environments. A minor but real operator-experience drawback also worked against PoshC2: interacting with an agent and viewing its output typically requires two separate console windows or tabs.

III. SLIVERC2

There is a recurring irony in this space: several of the most capable C2 frameworks were created and are maintained by security companies-Nettitude/LRQA, Bishop Fox, Fortra-and, although intended for adversary emulation, were well-crafted enough to be adopted by real threat actors. SliverC2 is a case in point. It was created by Bishop Fox and introduced in June 2019 as an open-source, Go-based C2 framework for red-team operations and penetration testing, gaining traction from around 2020 for modern features such as mutual TLS (mTLS) and dynamic code generation. It is actively maintained and released under the GPLv3 licence [2].

Sliver is modular and cross-platform, provides native binaries, and supports multiple C2 protocols including HTTP, HTTPS, DNS, and WireGuard. It generates a unique, dynamically compiled implant for each session [5], which complicates signature-based detection. Go has become popular in offensive security and is not yet as heavily instrumented at the host level as PowerShell. Sliver's 'Armory' package system supports extension, and several built-in enumeration commands deliberately avoid classic, well-signatured utilities such as whoami and systeminfo, instead using BOFs and Windows API calls to obtain equivalent information while reducing detection. Sliver also offers several mechanisms to limit or avoid the fork-and-run pattern that seasoned defenders watch for.

IV. COMPARATIVE ANALYSIS

To make the comparison rigorous rather than impressionistic, Table I contrasts the two frameworks across ten fixed dimensions. The discussion that follows interprets the differences that bear most directly on operator selection under present-day defensive pressure.

The most consequential difference is the runtime. PoshC2's reliance on PowerShell and .NET places its core activity on the most heavily instrumented execution surfaces of modern Windows, where transcription, script-block logging, AMSI, and CLM converge. Sliver's Go runtime sits on a less mature host-instrumentation surface and compiles to native binaries for Windows, Linux, and macOS, aligning with the cross-platform, cloud-and-hybrid [12]. For operations that must traverse non-Windows hosts, this is a decisive advantage, for Windows-only, Active-Directory-rich targets, PoshC2's mature AD tradecraft remains relevant.

Dimension	PoshC2	SliverC2
Developer & first release	Nettitude (now LRQA); released July 2016.	Bishop Fox; released June 2019.

Dimension	PoshC2	SliverC2
Implementation language / runtime	Server in Python 3; agents in PowerShell and C#/.NET.	Server and implants in Go (Golang), with cross-compiled native binaries.
Primary OS focus	Windows-centric; a Linux agent and BOF execution were added in v8 (2022).	Cross-platform by design: Windows, Linux, and macOS first-class targets.
Implant generation	Pre-built download cradles, shellcode, and droppers of several variants out of the box.	Per-session, dynamically compiled implants, frustrating static signatures.
C2 protocols	HTTP/HTTPS (encrypted), with proxy awareness.	HTTP, HTTPS, DNS, mTLS, and WireGuard.
Post-exploitation modules	Built-in Mimikatz, keylogging, AD enumeration, lateral movement via WMI/PsExec.	Modular 'Armory' package system; enumeration via BOFs and Windows API calls that avoid signed commands.
Detection surface (primary)	PowerShell, WMI/CIM, .NET reflection: technologies heavily instrumented on modern Windows.	Go runtime artefacts and large static binaries; less mature host-level instrumentation than PowerShell.
Fork-and-run posture	Module system relies on .NET reflection; reducing fork-and-run requires manual tuning.	Provides several mechanisms to limit or avoid fork-and-run execution.
Operator interface	CLI; interacting with an agent and viewing its output typically needs two windows/tabs.	Single console with both interactive and scripting (operator) modes.
License / maintenance	Open source; maintained by LRQA.	Open source (GPLv3); actively maintained by Bishop Fox.

PoshC2's strength of shipping ready-made cradles, shellcode, and droppers became a liability as those artefacts accumulated public signatures. Sliver's per-session dynamic compilation produces a distinct implant each time, which raises the cost of static, signature-based detection. This advantage is not unconditional: in its default configuration Sliver still leaves substantial host- and network-level footprints, and prevalence telemetry shows that default deployments remain detectable [6].

Both frameworks provide credential access, enumeration, and lateral movement. The differentiator is how that activity manifests to defenders. PoshC2's modules lean on .NET reflection and, where lateral movement uses WMI/PsExec, generate well-understood indicators. Sliver's use of BOFs and direct Windows API calls for enumeration, together with mechanisms to limit fork-and-run, is designed precisely to deny defenders those high-signal behaviours. This mirrors the broader migration toward in-process execution that Cobalt Strike's BOF model popularised.

Kaspersky's quarterly vulnerability-and-exploit reports publish rankings of the C2 frameworks most frequently observed in APT activity. Across 2025 these rankings consistently place Sliver in the top tier-among the most-used frameworks in the first half of the year, and holding the top position in the Q4 2025 analysis, ahead of Mythic and Havoc, [10], [11]. PoshC2 does not appear in these top-ranked lists. Independent vendor telemetry tells a complementary story: Red Canary identified Sliver, Mythic, and Brute Ratel as frameworks to watch as adversaries sought alternatives to more heavily detected tooling [13]. Taken together, the prevalence data substantiate Sliver's ascent to the front rank of observed C2 tooling while PoshC2 remains, at most, a secondary presence.

Beyond aggregate counts, specific intrusions document movement toward Sliver as established tooling became more detectable. Reporting links APT29 (associated with Russia's SVR) to Sliver for maintaining access following the SolarWinds intrusion, as noted in a 2021 NCSC advisory, a prolific ransomware affiliate tracked by Microsoft is reported to have migrated to Sliver as Cobalt Strike detection improved and the financially motivated actor TA551/Shathak distributed Sliver via macro-laden phishing [9]. The DFIR Report further documented Sliver deployed as a hands-on-keyboard payload ahead of ransomware in a 2024 intrusion [7]. The common pattern in these cases is migration away from tooling whose indicators defenders had learned, toward Sliver's lower-profile, cross-platform implants.

The strongest caution against an over-stated 'replacement' narrative comes from incident-response data. In August 2024 The DFIR Report analysed adversary infrastructure-active intermittently since at least September 2023-on which the operators used PoshC2 and Sliver together as their primary C2 toolkits, alongside Ngrok and SystemBC, in activity assessed with medium confidence as ransomware-related. This is direct evidence that PoshC2 was not discarded but retained as one component of a multi-framework toolkit. The honest reading of the combined evidence is therefore a reweighting-Sliver rising [8] to the front rank while PoshC2 persists in a situational, secondary role-rather than a clean one-for-one substitution.

C2-prevalence telemetry is subject to detection and sampling bias. Frameworks that are easier to detect, or that are run in default configurations, are over-represented relative to well-obfuscated or privately forked implants, conversely, heavily customised Sliver builds reported by incident responders may evade the very counts that rank Sliver highly. Vendor visibility also differs: telemetry weighted toward particular customer bases can rank Cobalt Strike or Metasploit above Sliver [14]. Several migration cases rest on secondary CTI reporting rather than primary disclosure. These rankings should therefore be read as directional rather than absolute, and the conclusions below are framed accordingly.

V. CONCLUSION

Is PoshC2 gone? No, it is still a great C2 framework by all means. Truth is modern offensive cyber operations

involve usually more than one tool and C2 frameworks are not an exemption. After gaining initial foothold, a smaller, dispensable, or more applicable frameworks and implants are used like Nimplant or PoschC2 and once internal enumeration, recon, privilege escalation and some sort of persistence is achieved the main tools and TTP's needed for introducing the operation actions on objectives and the intended effects (data exfiltration, defacement, data alteration and destruction, malware introduction, espionage and sabotage) are being brought in, be it another framework implant or living of the land utilities. Complex environments require complex tradecraft and higher level of operational security, since defenders focus is shifting from the lower levels of the David Bianco's Pyramid of Pain, IP, Hashes, Domains towards hunting tools and TTP's.

REFERENCES

- [1] S. Snape, "Introducing PoschC2 v8.0," LRQA Cyber Labs, 2022. [Online]. Available: <https://www.lrqa.com/en/cyber-labs/introducing-poshc2-v8-0/>. [Accessed: March 29, 2026].
- [2] Bishop Fox, "Sliver: A cross-platform adversary emulation framework," GitHub, 2023. [Online]. Available: <https://github.com/BishopFox/sliver>. [Accessed: March 30, 2026].
- [3] Microsoft, "How AMSI helps (Antimalware Scan Interface)," Microsoft Learn, 2023. [Online]. Available: <https://learn.microsoft.com/en-us/windows/win32/amsi/how-amsi-helps>. [Accessed: Apr. 04, 2026].
- [4] Microsoft, "PowerShell security features: Logging and transcription," Microsoft Learn, 2023. [Online]. Available: <https://learn.microsoft.com/en-us/powershell/scripting/security/security-features>. [Accessed: Apr. 02, 2026].
- [5] D. Bianco, "The pyramid of pain," Enterprise Detection & Response, Mar. 2013. [Online]. Available: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>. [Accessed: Apr. 02, 2026].
- [6] Kaspersky, "Vulnerability landscape in Q4 2025," Securelist, Mar. 2026. [Online]. Available: <https://securelist.com/vulnerabilities-and-exploits-in-q4-2025/119105/>. [Accessed: March 29, 2026].
- [7] The DFIR Report, "Threat actors' toolkit: Leveraging Sliver, PoschC2 & batch scripts," The DFIR Report, Aug. 2024. [Online]. Available: <https://thedfirreport.com/2024/08/12/threat-actors-toolkit-leveraging-sliver-poshc2-batch-scripts/>. [Accessed: Apr. 05, 2026].
- [8] The MITRE Corporation, "MITRE ATT&CK," MITRE ATT&CK, 2025. [Online]. Available: <https://attack.mitre.org/>. [Accessed: Apr. 02, 2026].
- [9] Fraunhofer FKIE, "APT29 - Threat actor profile," Malpedia, 2024. [Online]. Available: <https://malpedia.caad.fkie.fraunhofer.de/actor/apt29>. [Accessed: Apr. 05, 2026].
- [10] Kaspersky, "Vulnerability landscape analysis for Q2 2025," Securelist, Aug. 2025. [Online]. Available: <https://securelist.com/vulnerabilities-and-exploits-in-q2-2025/117333/>. [Accessed: Apr. 05, 2026].
- [11] Kaspersky, "Analyzing the vulnerability landscape in Q3 2025," Securelist, 2026. [Online]. Available: <https://securelist.com/vulnerabilities-and-exploits-in-q3-2025/118197/>. [Accessed: Apr. 06, 2026].
- [12] Mandiant, "M-Trends 2025: Data, insights, and recommendations from the frontlines," Google Cloud Threat Intelligence, Apr. 2025. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025>. [Accessed: March 30, 2026].
- [13] Help Net Security, "Attackers are handing off access in 22 seconds, Mandiant finds (M-Trends 2026)," Help Net Security, Mar. 2026. [Online]. Available: <https://www.helpnetsecurity.com/2026/03/24/mandiant-m-trends-2026-report/>. [Accessed: Apr. 05, 2026].
- [14] Red Canary, "C2 frameworks," Red Canary Threat Detection Report, 2025. [Online]. Available: <https://redcanary.com/threat-detection-report/trends/c2-frameworks/>. [Accessed: Apr. 05, 2026].

DCSync Attack from an Adversary Point of View

Dimitar Nikolov

IT Department

Nikola Vaptsarov Naval Academy

Varna, Bulgaria

d.nikolov@naval-acad.bg

Abstract – This paper examines the DCSync attack from an adversarial perspective, analysing its operational logic, execution variants, and the detection surface each variant presents within monitored Active Directory environments. The study was conducted in a controlled laboratory environment comprising a Windows Server 2019 domain and a monitoring stack including Wireshark, Suricata, and Windows Event Log auditing, enabling systematic comparison of five distinct execution approaches ranging from PowerShell in-memory execution and Mimikatz invocation to Beacon Object File deployment and Impacket-based execution from Linux hosts. Experimental results demonstrate that DCSync's widely assumed low-noise characteristic is method-dependent rather than inherent. Network traffic analysis identifies non-domain-controller source IP addresses, TTL values indicative of Linux origin, and the absence of Kerberos authentication as reliable detection indicators, while Windows Event ID 4662 provides complementary log-based coverage across all tested variants. The findings confirm that combined network, log, and protocol-level monitoring provides effective detection across the full range of execution paths, and position DCSync as a technique whose stealth is contingent on tooling selection, authentication protocol, and operational timing rather than on any intrinsic property of the attack itself.

Keywords – Active Directory, credential access, DCSync, detection, domain replication, operational security, privilege escalation, Windows security.

I. INTRODUCTION

DCSync is a stealthy attack geared towards gaining access to domain account NTLM password hashes via abuse of legitimate functionality used for data replication and synchronisation between domain controllers in an Active Directory environment [1]. The attack itself usually happens in the latest stages of a kill chain, when sufficient control and presence have been established in the environment. The attack leverages the Directory Replication Service Remote Protocol (MS-DRSR) [2] to extract credentials without running code on the target domain controller memory or directly compromising the NTDS.dit file. It requires a domain account with replication permissions, specifically Replicating Directory Changes

and Replicating Directory Changes All. These permissions are granted by default to the Domain Admins, Enterprise Admins, Administrators, and Domain Controllers groups, and the System account. Read-only domain controllers (RODCs) can also be targeted. The synchronisation is performed via a replication request utilising the DRSUAPI interface, specifically the GetNCChanges function - the same API call and mechanism used in legitimate domain controller to domain controller replication - which makes the attack fairly stealthy by design.

Legitimate replication calls between domain controllers happen frequently and can be triggered by changes to the Active Directory database, scheduled intervals, or manual administrative actions. Event-based triggers include urgent replication events such as account lockouts, changes to the LSA Secret, and PDC Emulator master changes [3], all of which bypass typical schedules and initiate immediate replication. Update notifications represent a further event-based trigger, whereby when a change is made the source domain controller notifies its replication partners after a short delay. If the Knowledge Consistency Checker creates a new connection object due to topology changes, replication is triggered as well. Scheduled triggers govern intra-site replication, which occurs automatically by default at five-minute intervals, and inter-site replication, which is scheduled by an administrator via site links and designed to manage bandwidth usage. Administratively initiated replication can be triggered voluntarily by any user with access to an account holding the required permissions. System event triggers include domain controller boot and promotion events, both of which initiate synchronisation via Server Manager or PowerShell to ensure the controller is up to date before accepting client requests [4].

All the above demonstrates that legitimate replication happens fairly often - at least once every five minutes - but still adheres to a rhythmic pattern to a certain extent. This is operationally significant since this rhythm affects offensive operational security choices and simultaneously creates the baseline for identifying anomalous behaviour during threat hunting [6].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.213>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

II. DCSYNC ATTACK CHAIN

The DCSync attack chain consists of four sequential steps, each carrying distinct operational security considerations. The first step requires taking over or creating an account capable of triggering replication. Most of the default accounts holding these permissions reside on the domain controller, which is a highly monitored area and a position an offensive operator should seek to avoid. The preferred strategy is hunting for domain users or weak service accounts that have been additionally granted replication permissions. BloodHound, SharpHound, and ACL manipulation [5] are the paths most commonly taken at this stage, typically in combination with other lateral movement techniques [7].

The second step involves locating the target domain controller. One of the less operationally secure approaches is skipping proper host enumeration and performing a scan. Regardless of how well configured, a scan is an action that is well signatored and carries a risk of disclosing the operator's current position. Since all domain-joined machines communicate almost constantly with the domain controller, it is quite often sufficient to monitor network traffic, check logs and caches, or perform a simple DNS resolve or network configuration query to locate the domain controller without generating anomalous activity. The third step is sending the replication request. Numerous tools are capable of sending a replication request and receiving the resulting hashes, including Mimikatz in all of its forms and variants, Impacket, PowerShell, and built-in utilities in most popular C2 framework implants and beacons. All of these require authentication material and an account with replication permissions. The fourth and final step is utilising the retrieved hashes to move laterally, vertically, or to act on operational objectives. This step is also one of the determining factors in what constitutes the best tooling choice in the previous step, since different downstream applications impose different requirements on the format and completeness of the extracted credential material.

The techniques and tools most commonly used at step three each carry distinct trade-offs. PowerShell-based implementations, such as the Invoke-DCSync scripts available from pentestfactory and S3cur3Th1sSh1t, pull Mimikatz, PowerView, and ADRecon from GitHub into memory and perform DCSync without writing primary tooling to disk. The S3cur3Th1sSh1t variant additionally extracts the krbtgt password, builds a Golden Ticket, imports it, and adds a specified account to the Enterprise Admins group in a single execution chain, though it does output multiple files to disk [8]. To reduce detection risk, scripts should be staged on a payload server within offensive infrastructure, protected where possible by redirectors, and executed on a softened legitimate Active Directory machine with detection and logging disabled - ideally a new or compromised domain controller, which aids in blending with legitimate replication traffic.

Mimikatz remains one of the most widely used tools for DCSync execution. Synchronisation of all domain accounts should be avoided, as the /all flag produces a measurable peak in network traffic and is operationally

unnecessary given that sufficient access has already been established by the point DCSync is employed. Targeted extraction of specific high-value accounts is the preferred approach. SafetyKatz, a combination of a slightly modified Mimikatz build and a .NET PE Loader created by Will Schroeder of SpecterOps, provides equivalent capability with improved evasion characteristics.

A Beacon Object File represents the most operationally secure execution path for DCSync where a C2 implant is already established on the target machine. A BOF is a compiled C program written to a convention that allows it to execute within a beacon or implant process and use internal beacon APIs, extending the agent with new post-exploitation features without spawning new processes visible to monitoring tools. Initially an exclusively CobaltStrike feature, BOF execution has been widely adopted across modern C2 frameworks including PoshC2, Sliver, AdaptixC2, and Havoc. Since most current C2 implants operate as fileless malware running entirely in memory, and since BOF execution inherits the implant's existing unhooking and alternative API call mechanisms, this approach minimises both disk and process-level detection vectors. Mimikatz, SafetyKatz, Kiwi, and Invoke-DCSync all exist as assemblies or are implemented directly within C2 agent frameworks [9].

Impacket's secretsdump.py provides DCSync capability from a Linux host and is not recommended in well-monitored environments, as the detection section of this paper demonstrates it presents multiple observable indicators. If used, Kerberos ticket authentication is strongly recommended. In DCSync attacks, different authentication mechanisms and protocols can be employed, including Kerberos, MS-RPC, and SMBv3. Kerberos ticket authentication represents the common secure baseline, and any deviations - including plaintext passwords, pass-the-hash using NTLMv1 hashes, or raw SMB authentication - are outliers that should be considered operationally unsafe.

III. DETECTION OF THE DCSYNC ATTACK

Detection of DCSync [10] activity is most effective when network monitoring, Windows event log correlation, and protocol-level analysis are deployed in combination, since no single indicator provides reliable coverage across all execution methods. Each layer of detection addresses a different subset of the attack surface, and their convergence produces a high-confidence detection posture that is resistant to the operational security measures an adversary is likely to employ.

The primary log-based detection signal is Windows Event ID 4662 [11], generated when a principal exercises an extended right against a directory object. Specifically, the appearance of the GUID 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 - representing the control access right for Replicating Directory Changes All - in a 4662 event indicates that a replication operation has been performed against the directory. The analytical value of this indicator depends on the identity of the account triggering the event. Any account outside the Domain Controllers, Domain Admins, and Enterprise Admins groups generating this event represents an anomaly that warrants immediate

investigation [12]. In environments where replication permission grants are properly controlled and audited, this indicator carries a high signal-to-noise ratio and a low false positive rate.

Network monitoring and traffic analysis represent the most reliable and method-independent detection layer, capable of identifying DCSync activity regardless of the tooling used by the attacker. The first and most actionable network indicator is source IP anomaly: DsGetNCChanges replication requests originating from IP addresses outside the designated domain controller subnet are inherently anomalous, since in a correctly configured environment only domain controllers initiate replication requests. A detection rule implemented in an intrusion detection or prevention system such as Snort or Suricata, configured to alert on DsGetNCChanges [13] requests from non-domain-controller IP addresses, provides a high-fidelity detection signal with minimal tuning overhead. Fig. 1 illustrates a captured DsGetNCChanges request from a non-domain-controller host, showing the source IP and DRSR protocol identifier that together provide the basis for this detection rule.

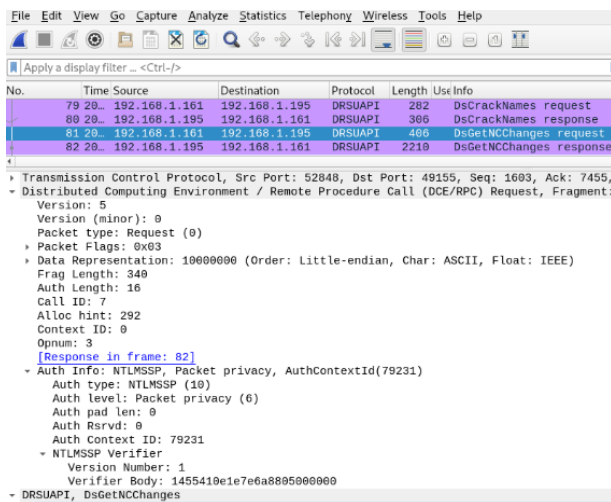


Fig.1. DsGetNCChanges Request.

The second network indicator is TTL-based operating system fingerprinting. Examination of the IP TTL value in replication request packets provides a reliable method for identifying the origin operating system of the requesting host. A TTL value of 64, as illustrated in Fig. 2, is characteristic of Linux default IP stack behaviour and is distinctly different from the TTL of 128 produced by Windows hosts. When a DsGetNCChanges request originates from an IP address outside the domain controller subnet and carries a TTL of 64, the combination provides a highly specific detection signature for Impacket-from-Linux executions without requiring deep packet inspection or protocol decryption.

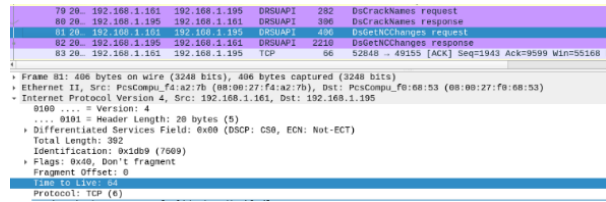


Fig. 2. DsGetNCChanges Request TTL 64

The third network indicator is protocol composition anomaly. In a correctly functioning Active Directory environment, all domain controller to domain controller replication sessions include Kerberos authentication as part of the session establishment. Protocol analysis of traffic associated with Impacket NTLM-authenticated DCSync executions reveals a session composed entirely of SMB2 [14] traffic with no corresponding Kerberos exchanges, as illustrated in Fig. 3. The complete absence of Kerberos traffic in a replication session is a high-confidence anomaly that is straightforwardly detectable through protocol distribution analysis of captured traffic. It should be noted that Windows-based executions using Mimikatz or BOF methods authenticate via Kerberos by default, producing session profiles that are consistent with legitimate replication and substantially reducing the value of this indicator for those specific methods [15].

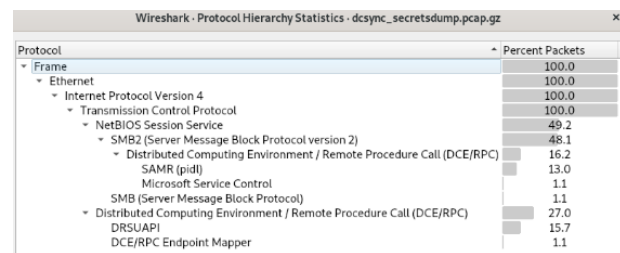


Fig. 3. SMB2 DCSync.

The three indicators together - non-domain-controller source IP, TTL value of 64, and SMB-only protocol composition absent Kerberos - form a highly specific composite signature for the use of Impacket from a Linux host to execute DCSync following lateral access to the local network segment. The convergence of all three in a single captured session, as observed in the laboratory environment, reduces the probability of false positive classification to negligible levels. The fourth network indicator is traffic volume anomaly. Full domain synchronisation executions, extracting all account hashes simultaneously, produce a measurable spike in DRSR traffic volume relative to the established replication baseline, as illustrated in Fig. 4. This peak is both unnecessary from an operational perspective - since targeted extraction of high-value accounts provides equivalent leverage - and avoidable, representing an operational security failure that significantly increases detection probability.

Protocol decryption capabilities substantially enhance detection coverage across all execution methods, including Windows-based approaches that otherwise produce network profiles consistent with legitimate replication. The DCSync attack relies on a number of Microsoft protocols including Kerberos, MS-RPC, and SMBv3, all of which

employ encryption in default enterprise configurations. Security monitoring tools equipped with decryption capabilities for these protocols can perform early detection of abnormal behaviour within encrypted sessions, including the identification of forged Kerberos tickets and anomalous MS-RPC call patterns that would otherwise be invisible to signature-based network detection. Protocol decryption should therefore be considered an essential capability for any security monitoring architecture deployed in environments where Active Directory credential theft represents a credible threat scenario.

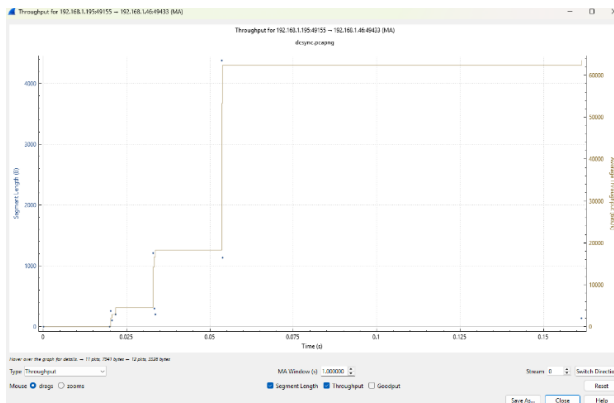


Fig.4. DCSync all request traffic peak.

IV. CONCLUSION

DCSync represents a high-value technique in the final stages of Active Directory compromise, offering an adversary the ability to extract domain credential material without direct interaction with domain controller memory or the NTDS.dit database. Its operational value, however, is contingent on the disciplined application of sound operational security practices at every stage of its execution chain - from privilege acquisition and domain controller location through tooling selection, authentication protocol choice, and the scope of the replication request itself. The experimental findings presented in this paper confirm that DCSync's reputation as an inherently low-noise technique is method-dependent rather than absolute, and that operationally careless execution - particularly through Impacket from a Linux host using NTLM authentication, or through full-domain synchronisation - produces a distinctive and reliably detectable forensic signature across network, log, and protocol monitoring layers simultaneously.

DCSync is most correctly understood not as a terminal objective but as an enabling technique whose primary value lies in what it makes possible downstream. Its strongest application is as a component of Kerberos-based persistence strategies, where the credential material it yields - most critically the krbtgt hash and targeted service account hashes - enables the fabrication of Golden, Silver, Diamond, and Platinum tickets, providing an adversary with durable, difficult-to-remediate Enterprise Admin-level persistence within the domain. It is within this broader strategic context that DCSync's risk profile must be evaluated: the operational security investment required to execute it stealthily is justified precisely by the long-term

persistence and privilege it unlocks, and any execution approach that compromises stealth for convenience undermines the very objective the technique is intended to serve.

REFERENCES

- [1] Invoke-DCSync, "Invoke-DCSync Linux Implementation." [Online]. Available: <https://github.com/pentestfactory/Invoke-DCSync/tree/main/linux> [Accessed: Mar. 26, 2026].
- [2] ViperOne, "Credential Dumping: NTDS." [Online]. Available: <https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/credential-access/credential-dumping/ntds> [Accessed: Mar. 25, 2026].
- [3] ViperOne, "DCSync Attack." [Online]. Available: <https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/credential-access/credential-dumping/dcsync/dcsync-attack> [Accessed: Mar. 26, 2026].
- [4] 0xss0rz, "DCSync Attack (Internal Pentest)." [Online]. Available: <https://0xss0rz.gitbook.io/0xss0rz/pentest/internal-pentest/dcsync> [Accessed: Mar. 26, 2026].
- [5] W. Uentin, "InvokeRogueDC Tool." [Online]. Available: <https://github.com/Wuentin/InvokeRogueDC> [Accessed: Mar. 26, 2026].
- [6] D. Dimitrov et al., "The Risk of Personal Smart Devices in the Operational Security for Military Bases, Personnel and Missions," Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, vol. 2, pp. 99–106, Jun. 2025, <https://doi.org/10.17770/etr2025vol2.8616> [Accessed: Mar. 26, 2026].
- [7] U. Ravindran, "AD Series: DC Sync Attacks," Medium, 2023. [Online]. Available: <https://medium.com/@urshilaravindran/ad-series-dc-sync-attacks-e76bb54308f5> [Accessed: Mar. 28, 2026].
- [8] Active Directory Security, "Mimikatz DCSync Detection," Oct. 2018. [Online]. Available: <https://www.active-directory-security.com/2018/10/mimikatz-dcsync-detection.html> [Accessed: Mar. 28, 2026].
- [9] N. Vladimirova and D. Dimitrova, "Simulation of a LoRa-Based Wearable System for Maritime Emergency Tracking Using MATLAB," in Proc. 19th Int. Conf. on Communications, Electromagnetics and Medical Applications (CEMA'25), Athens, Greece, 2025, pp. 16–20. ISSN: 1314-2100. [Online]. Available: http://rcvt.tu-sofia.bg/CEMA/proceedings/CEMA_2025_proc.pdf [Accessed: Mar. 28, 2026].
- [10] Netwrix, "What is DCSync: An Introduction." [Online]. Available: <https://netwrix.com/en/resources/blog/what-is-dcsync-an-introduction/> [Accessed: Mar. 15, 2026].
- [11] ExtraHop, "DCSync Attack Overview." [Online]. Available: <https://www.extrahop.com/resources/attacks/dcsync> [Accessed: Mar. 29, 2026].
- [12] D. Dimitrov and E. Andreev, "China's Strategic Competition in Cyberspace: Volt Typhoon and Salt Typhoon as a Projection of Power, a More Aggressive Posture and a Future Beyond Espionage," Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, vol. 2, pp. 115–122, 2025. Available: <https://doi.org/10.17770/etr2025vol2.8618> [Accessed: March 28, 2026].
- [13] Altered Security, "A Primer on DCSync Attack and Detection." [Online]. Available: <https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection> [Accessed: Apr. 05, 2026].
- [14] W. Schroeder, "SafetyKatz Credential Extraction Tool," GhostPack, 2018. [Online]. Available: <https://github.com/GhostPack/SafetyKatz> [Accessed: Apr. 05, 2026].
- [15] P0142, "DCSync Beacon Object File." [Online]. Available: <https://github.com/P0142/DCSync-Bof> [Accessed: Apr. 05, 2026].

A Multilayer Framework for Urban Microclimate Analysis in Smart Sustainable City Design: The Vienna Case

Nikolay Nikolov

Department of Physics,
University of Architecture, Civil Engineering and Geodesy,
Sofia, Bulgaria

ORCID:

0009-0000-6989-5832
niki.nikolow87@gmail.com

Iliyan Vasilev

Sofia University Kliment Ohridsky
Sofia, Bulgaria

ORCID:

0009-0008-0863-1516
ilias.vasilidis@gmail.com

Abstract—This paper presents a Vienna-focused conceptual framework for urban microclimate analysis in smart sustainable city design. The study is based on a targeted review of microclimate monitoring approaches, GIS-based morphology indicators, and simulation workflows, which is used to identify recurring limitations and translate them into a multilayer structure. This framework models how morphological parameters (urban morphology and sky view factor) of urban terrain influence variability of microclimate. In more detail, the framework utilizes energy-simulation and intelligent management layers to address the problems of local weather files that lead to a climate gap, limited interaction between buildings and the surrounding microclimate, and the fragmentation between GIS layers and engineering tools. The framework enables spatially informed climate adaptation strategies as well as data-driven planning in smart sustainable cities. The proposed framework provides a transferable methodological tool for climate-responsive urban planning and design.

Keywords— urban microclimate, urban morphology, GIS, spatial variability, sky view factor.

I. INTRODUCTION

The concept of smart and sustainable cities is considered a contemporary challenge of the 21st century. Metropolises today face a wide range of challenges [1]. These include rapid urbanization, demographic pressure, migration flows, air pollution and socio-economic disparities [2], as well as broader geopolitical tensions. In this context, smart cities rely on information and communication technologies to support sustainable growth and improve social and economic well-being [3]. In this paper, the term ‘smart city’ is used consistently, following the terminology of the cited authors, although in the literature it is sometimes used interchangeably with

‘intelligent city’. Smart city thinking has evolved alongside technological progress. One of the most influential frameworks is that of Giffinger et al. [4], who identify six key dimensions of a smart city (Fig. 1). According to Giffinger et al. [4], a smart city is called one that has advanced characteristics for economy, mobility, environment, people, lifestyle and management.



Fig. 1. Characteristics and factors of a smart city (Source: Adapted from Giffinger [4])

In this way, an intelligent combination of factors is created that contribute to promising development based on local

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.29>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

circumstances and activities carried out by politics, business and residents [4].

Petrova-Antonova argues that “smart” cities are grounded in data and people, with technology serving as a means rather than an end [5], [6]. The emphasis falls on citizens, as a smart city should ultimately work to optimise resources for their benefit. The concept of the digital twin [7], [8] provides a basis for sustainable planning. Mapping and simulation become tools for testing design options and assessing their impact on the urban environment. Digital twins are not just 3D models, but living simulation systems that help to understand how any change will affect other urban systems. Petrova-Antonova et al. [5],[6] emphasize that by raising the hypothesis that a “smart” city is not just technological digitalization, but a significant optimization of processes to achieve correct and sustainable solutions for the benefit of citizens. Georgieva argues that smart cities should be understood not only as technological systems but also as economic and managerial transformations. Her framework is built around three pillars: smart governance, innovation systems and sustainable competitiveness [9]. According to her overall concept, a smart city is considered to be a polis that contains in its urban planning architecture effective resource management, and in this regard, technologies become a means of achieving transparent policies for and towards citizens in the process of making managerial decisions [9]. A city becomes “smarter” when it links science, business and local government into a shared innovation ecosystem, following the Triple Helix model [10]. The scientist emphasizes the importance of innovation ecosystems and the need for new models for smart governance in order to achieve urban sustainability [9]. In this context, the sustainability of innovation ecosystems depends directly on the effective management of technological obsolescence, which ensures that implemented innovations will perform their functions throughout their life cycle [11]. These perspectives by Petrova-Antonova et al. [5], [6], [8] and Georgieva et al. [9] provide the conceptual foundation for integrating governance, data and citizen-centric approaches within smart city systems.

The transition from the Triple Helix [10] to the Quintuple Helix expands the model by adding civil society and the natural environment as core components. This is a key moment that unites the concepts of intelligent (technology and people) with sustainability (environment). The role of civil society [12] as a construct is significant for the formulation and implementation of ideas in the context of innovations, which are a reflection of culture and a specific way of life. The term ‘Quintuple Helix’ is used in this study to denote the five interacting subsystems of innovation, following Carayannis and Campbell [13]. The ecological imperative, embedded in the Quintuple Helix as a critical fifth element, contributes to the highest form of the model and places the innovation system in the context of environmental protection. Focus is placed on climate change and the preservation of natural capital in the service of society, as a driver of innovation processes. Fig. 2 illustrates the systems in the context of the Quintuple Helix,

which Carayannis & Campbell call nested systems [14],[15].

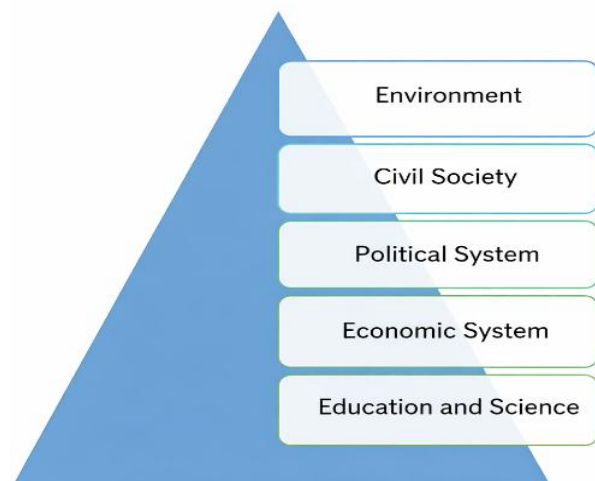


Fig. 2. Conceptual interaction model of the Quintuple Helix in a smart sustainable city

The Quintuple Helix model conceptualizes innovation as a non-hierarchical system of interacting subsystems, including academia, industry, government, civil society and the natural environment [13–15]. These components function as mutually interdependent actors within a dynamic innovation ecosystem rather than as a linear or hierarchical structure. Accordingly, Fig. 2 is reinterpreted not as a hierarchy but as a conceptual interaction model, where each subsystem contributes to and co-evolves with the others in the context of smart and sustainable urban development.

However, these subsystems should be viewed as connected, and not hierarchical. The education and research sub-system will provide the capacity for knowledge and innovation, whereas the economic sub-system will convert the knowledge into solutions. The political sub-system will guide the rules and strategy for implementation, the civil society sub-system will guarantee social involvement, and the natural environment will define the ecological boundaries for smart and sustainable cities.

There is a substantial amount of research on both urban microclimates and smart-city development, but the two fields often move in parallel rather than together. This separation creates what many planners describe as a “climate gap”, especially when simplified weather files are used in design and energy modeling. This paper outlines a multilayer framework that brings several strands of analysis into one structure: urban form, local microclimatic processes, energy performance and governance considerations. The idea is to account for spatial variability more explicitly, using indicators such as the Sky View Factor (SVF), building configuration and ventilation routes, all of which shape local thermal conditions. Vienna is used as a reference case, as it has well-developed climate monitoring practices and integrated urban planning policies, making it a suitable example for climate-responsive urban design.

II. METHODOLOGY

The methodology is structured in several steps: literature search, identification of gaps, comparison of existing approaches, framework development and pilot illustration.

A. Literature search strategy

The review relied on searches in Scopus, Web of Science and Google Scholar. Approximately 120 publications were identified through keyword combinations related to urban microclimate, UHI, SVF, energy simulation and Vienna. Applying relevance and quality criteria reduced the set to 48 studies that were examined in detail.

This study develops a multilayer conceptual framework based on a targeted review of scientific literature and policy documents on the topics of urban microclimate, UHI, urban morphology (U2O/SVF), energy simulations and smart governance, with a focus on Vienna. The paper generally takes a conceptual research method through a systematic review of scientific literature, policy documents, and planning practices. The framework put forward does not intend to be empirically checked at this stage. It rather combines fragmented analytical layers into a cohesive structure that can be used for scenario testing and pilot applications in the future.

The thematic search using keywords such as “urban microclimate”, “urban heat island”, “U2O”, “SVF”, “energy simulation”, “Vienna”, “digital twin” assisted in finding the sources, which were mainly chosen from peer-reviewed publications and official institutional materials. The various methods that had been chosen were initially categorized (e.g., monitoring/observations, GIS and morphological indicators, microclimate models, energy simulations, and management measures) and then the recurring limitations and gaps were identified (e.g. climate gap, limited building-microclimate feedback, fragmentation between GIS and engineering tools). Based on these, the gap-solution logic was followed and a multilayer framework (morphology - microclimate - energy simulation - intelligent control) was derived, intended for scenario planning and empirical testing thereafter.

B. Background on microclimate models (Vienna context)

Research analyses of the microclimate of Vienna have generally focused on the five-level framework and the urban heat island effects [16],[17] (density, materials, vegetation, comfort), and studies have shown that the above factors influence urban planning and environmentally friendly decision-making in order to improve the sustainability of the urban area and to prevent global climate change [18],[19]. Microclimatic variations in urban areas have been found to affect metropolitan areas on a local and global scale, with direct consequences for the health of people living in cities [20],[21]. Microclimatic conditions can vary significantly due to the specificities of the urban fabric. Scientists have introduced the term urban unit of observation (U2O) [22] in order to systematize the

degrees of microclimatic diversity in urban areas [23] emphasizes the role of scale in microclimate studies, and for microclimate parameters to be measured correctly, the size of the sample area should not exceed a few hundred meters in radius.

Urban climatologists characterize the morphology of the city in terms of the height, width, and density of buildings, where the sky visibility factor is defined [24]. These properties affect the loss of longwave radiation at night and therefore the cooling rate, the access of sunlight during the day and thus the daily heating regime, as well as the air flow and wind speed at street level. The SVF factor for determining incoming and outgoing radiation as a heating and cooling model is shown in figure 3.

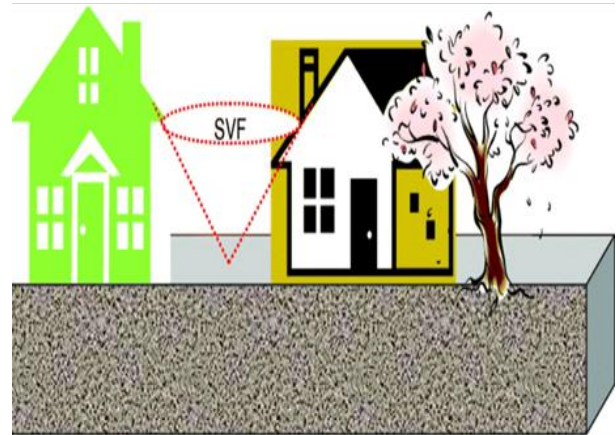


Fig. 3. SVF factor for determining incoming and outgoing radiation as a heating and cooling model [24]

The Sky View Factor (SVF) is an important parameter that influences the potential for radiative cooling and ventilation in densely built-up urban areas [25]. It forms a critical layer in the morphological analysis of U2O because it shows how effectively the urban environment can release accumulated heat through long-wave radiation. Lower SVF values are directly associated with stronger urban heat island effects. The key emphases that are placed in the development of the multilayer conceptual framework for improving architectural and landscape interventions are:

- 1) integrated approach – in addition to meteorological components, the strategy includes urban planning, green infrastructure and healthcare;
- 2) district-level measures – specific areas in Vienna are analyzed at the level of a separate observation unit in order to determine the so-called Cooling Hotspots;
- 3) SVF optimisation – improving sky visibility is applied as a method for natural cooling in densely built-up streets.

Vienna has an overview map of selected areas, each with one stationary meteorological station and two nearby locations for short-term mobile microclimate monitoring, attached in Fig. 4.

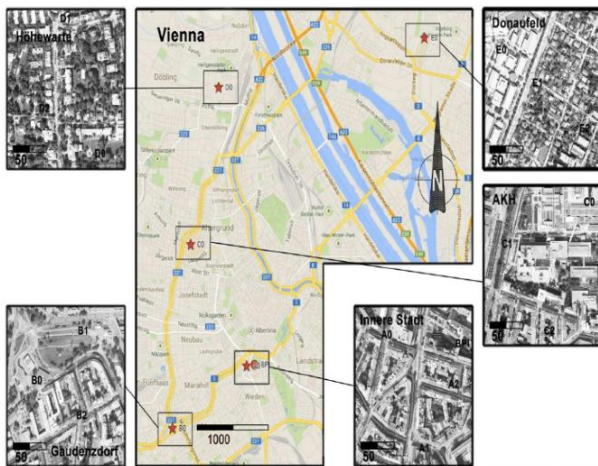


Fig. 4. Selected locations for visualization of mobile climate monitoring in Vienna in terms of air temperature, relative humidity, wind speed [27]

The results show that the temperature data from mobile monitoring stations located in the urban canyon are generally higher than the simultaneously measured data from meteorological stations [27]. Vuckovic et al.[28] conducted simulations of the thermal performance of buildings using the special EDSL TAS software due to its ability to systematically evaluate the thermal behavior of buildings while taking into account a relatively wide range of factors, such as complex building shapes, shadow effects between buildings, multi-zone building modeling, and integrated natural and forced airflow. Typical building floor plans are shown in figure 5.

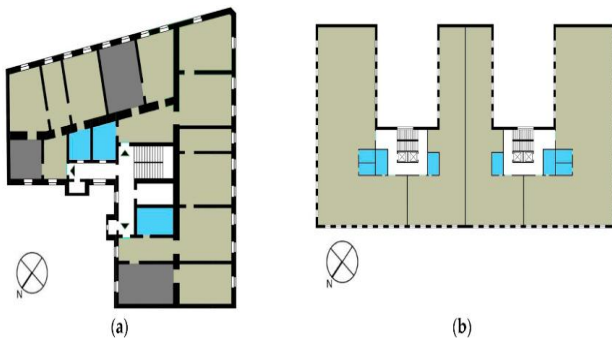


Fig. 5. Typical building floor plans [28]

According to Austrian standards, the authors of the study examined six components such as weather conditions, location specifics, ventilation, solstice.

C. Limitations and Identified Gaps

Based on the reviewed studies, an energy simulation layer is included in the proposed framework, as microclimatic conditions are closely related to building energy performance. Vuckovic et al. [28] point out that despite the ground-breaking research going on in Vienna, the problem lies mainly with the low spatial resolution of the climate data and the absence of a connection between microclimate variations and energy simulations. These limitations require the development of a multilayer conceptual framework that would overcome the

fragmented approach and provide a precise interface between urban morphology and the energy efficiency of buildings

In order to build a multilayer conceptual framework, the identified gaps and limitations need to be addressed, as follows:

- 1) "Climate gap" – the use of averaged meteorological data from suburban stations (airports) leads to errors in energy simulations of up to 16%. Buildings in the city center are designed with inaccurate parameters for summer heat load [28].
- 2) Lack of dynamic feedback – energy models consider the building as a passive object, without taking into account how it itself changes the microclimate around it (heat released by facades and air conditioners) [27].
- 3) Static material data – GIS models of Vienna are geometrically detailed, but lack dynamic data on albedo and thermal mass of urban surfaces [26].
- 4) Methodological fragmentation – there is no integrated software interface that automatically connects microclimatic layers with engineering tools for building design [17].

To better position the proposed framework within the existing literature, Table I presents a simplified comparison of commonly used approaches in urban microclimate analysis.

TABLE I. COMPARISON OF COMMON APPROACHES IN URBAN MICROCLIMATE ANALYSIS (SOURCE: AUTHORS)

Approach	Main focus	Limitation
Urban morphology and GIS-based analysis [22–24]	Spatial structure and SVF	Limited interaction with dynamic microclimate processes
Microclimate studies and UHI analysis [16], [20], [27]	Local climate variability	Weak connection to building energy performance
Energy simulation models [28]	Building energy demand	Often based on generalized weather data.
Proposed multilayer conceptual framework (this study)	Integration of morphology, microclimate and energy simulation	Closes the "climate gap" by linking spatial morphology with dynamic building performance.

As shown in Table I, most existing approaches address individual aspects of urban climate analysis, while the proposed framework attempts to combine them into a unified structure.

The gaps are displayed in a Table II, which serve to build a multilayer conceptual framework (solution):

TABLE II. GAP-SOLUTION LOGIC FOR DEVELOPING THE MULTILAYER CONCEPTUAL FRAMEWORK (SOURCE: AUTHORS)

Identified gaps	Solution
Climate Gap (16% error in energy projections)	Using local U2O data instead of suburban stations

Lack of feedback (building-microclimate)	Integration of dynamic energy simulation
Static albedo/material data	Digital layer with thermal properties of surfaces
Methodological fragmentation	Multi-layer structure combining GIS and engineering

Based on the methodological analysis, the multilayer framework is proposed as a conceptual structure that follows a logical flow from data to solutions, linking static urban strategies with dynamic scientific evidence. It is designed to fill the “climate gap” by integrating GIS, microclimatic data and energy simulations. Table III presents the conceptual structure of a multilayer conceptual framework.

TABLE III. CONCEPTUAL STRUCTURE OF A MULTILAYER CONCEPTUAL FRAMEWORK (SOURCE: AUTHORS)

Analysis Layer	Key Parameters and GIS Attributes	Main Contribution to the Model
1.Urban Morphology (U2O)	Building density, Sky View Factor (SVF), building height.	Defining the territorial unit for observation using OGD data.
2.Microclimatic Variations	Temperature amplitudes, albedo, wind corridors, humidity.	Identifying local thermal anomalies relative to the urban fabric.
3.Energy Simulation	Heat load, cooling needs, energy deficit of buildings.	Overcoming the “Climate Gap” and 16% error in forecasts.
4.Intelligent Management	Blue-green infrastructure, dynamic shading, Cooling Hotspots.	Formulating sustainable adaptation strategies in real time.

D. Multilayer Framework Development

The pilot analysis focuses on representative urban typologies in Vienna, specifically inner-district street canyons (e.g., typical Gründerzeit blocks) and adjacent open urban spaces. These typologies are selected as illustrative cases rather than fixed geographic coordinates, due to the conceptual nature of the study. Thus the pilot analysis was conducted to demonstrate how the proposed multilayer framework can be operationalized by linking urban morphology - expressed through the sky view factor (SVF) - to measurable microclimatic variations within Vienna. Two very different urban units of observation (U2O) were chosen: (1) a compact perimeter-block street canyon in the inner districts, and (2) an adjacent open square with much more sky visibility. By comparing these different cases, the influence of morphological variations on local thermal behaviour is demonstrated.

Examinations of Vienna reported a great extent of elevated air temperature of residential areas in the dense street canyons as opposed to the nearby open areas. This is taken to be the result of less longwave radiative cooling and limited ventilation in these street canyons. Mobile climate monitoring in Vienna also verifies this observation as it reveals that the street canyon temperatures were consistently higher than the temperatures measured by the

reference stations. As stated in the present paper, “The results show that the temperature data from mobile monitoring stations located in the urban canyon are generally higher than the simultaneously measured data from meteorological stations [29]. This corresponds to the findings of Kiesel, Vuckovic and Mahdavi, who observed significant microclimatic variability across different districts of Vienna, strongly influenced by building density, material properties and sky openness [30].

Vienna Urban Heat Island Strategy Plan (UHI-STRAT) identifies the creation of ventilation corridors and reducing heat build-up in dense areas as top priorities [31]. In alignment with these strategic objectives, this study employs the Sky View Factor (SVF) as a morphological indicator, drawing on established microclimatic research for Vienna that links low SVF to reduced ventilation and higher nocturnal heat retention [28, 30]. This scientific evidence complements the policy focus of UHI-STRAT by providing a diagnostic tool for identifying areas where cooling interventions are most needed.

For this pilot illustration, representative SVF values were derived from GIS-based morphology for the two U2Os. Dense street canyons in Vienna typically exhibit SVF values of approximately 0.25–0.35, while open squares and wider intersections reach SVF values of 0.70–0.80. Investigation of Vienna's urban climate finds that at night, the temperature can differ by several degrees Celsius between morphological types, with areas having a lower SVF (sky view factor) holding more heat after sunset [24], [30]. Such UHI patterns agree with the broader European research and also with the mobile monitoring results mentioned above.

The indicative relationship between SVF and local microclimate is summarized in Table IV. The values presented in Table IV are derived from a synthesis of reported ranges in the literature on Vienna's urban morphology and microclimate studies [24], [28], [30].

TABLE IV. INDICATIVE RELATIONSHIP BETWEEN SVF AND MICROCLIMATIC BEHAVIOUR IN TWO VIENNA U2OS (SOURCE: AUTHORS)

U2O type	Approx. SVF	Typical nocturnal air temperature behaviour
Dense street canyon	0.25–0.35	Higher nighttime temperatures; reduced longwave cooling; intensified UHI
Open square / less dense area	0.70–0.80	Lower nighttime temperatures; more effective radiative cooling; mitigated UHI

This pilot analysis operationalizes the first two layers of the proposed framework - urban morphology (U2O, SVF) and microclimatic variation - by linking a simple morphological indicator to local thermal behaviour. It also reinforces the relevance of the energy simulation layer. As noted earlier in the paper, the difference in the annual

heating load between different locations in Vienna can reach 16.1 kWh/m² per year. This indicates the relevance of integrating morphology-driven microclimatic variability into building performance assessment. The pilot SVF-based analysis provides a direct bridge to the intelligent management layer. The UHI-STRAT Vienna strategy has already a leading line urban ventilation corridors, shading and blue-green infrastructures. By integrating SVF-based diagnostics within this strategic framework, it enables locating Cooling Hotspots and thus first of all the top interventions in the areas where low SVF and high night temperatures coincide.

The pilot analysis is intended as an initial application example rather than a full empirical case study. It demonstrates how the proposed framework can be used to interpret real urban conditions based on representative typologies and literature-based data. In this sense, the analysis provides an initial form of methodological validation, as the framework is applied to cases that are consistent with empirically observed microclimatic patterns reported in previous studies.

This study puts forward a multilayer conceptual framework that functions as an integrative methodological structure rather than an empirical model or software tool. Its purpose is to link four analytical dimensions—urban morphology, microclimate, energy simulation and intelligent management—into a single workflow that can support climate-responsive urban planning. Although the framework is conceptual, the individual steps are described clearly enough to allow others to follow the same logic, replicate the approach and build on it through future empirical testing.

The described workflow can be replicated in other urban contexts, provided that comparable datasets, GIS-based indicators and locally collected microclimate measurements are available. The illustrative example presented here shows how the framework can be applied to identify areas with increased heat accumulation and to support targeted, climate-responsive interventions at the district scale.

III. DISCUSSION

The findings of the literature synthesis and pilot analysis highlight several key implications for urban climate-sensitive planning.

1) Critical influence of the local context – the microclimate varies significantly within the same city depending on the morphology (shape and density of buildings) and the materials used. Using common, standardized weather files (e.g. from the airport) for the entire city leads to serious design errors;

2) Effect on the energy efficiency of buildings – local weather conditions directly change the energy needs of buildings:

- the difference in the annual heating load between different locations in Vienna can reach 16.1 kWh/m² per year;

- a building with an identical construction will consume a different amount of energy just because of which district of Vienna it is located in.

3) Correlation between morphology and heat – strong relationships between built environment characteristics and microclimate are confirmed:

- building density – high building density is directly related to higher temperatures (intensification of UHI).

- materials – the properties of materials (albedo, thermal mass) in an urban unit influence how long heat is retained at night.

4) Need for site-specific data – for sustainable urban design, the researchers believe that site-specific meteorological data should be used, rather than average values. They propose a systematic framework for identifying the properties of the built environment (geometric and material) that influence these variations.

5) Health and comfort consequences – changes in the microclimate at the local level have immediate consequences for outdoor thermal comfort and the health of citizens, with these effects being most noticeable in densely built-up historical or industrial areas of Vienna.

The connection between the multilayer conceptual framework and the Quintuple Helix can be seen clearly when viewed through the five subsystems:

1) Educational system – the academic research of Lim et al. [27] defines the theoretical framework for the analysis of temperature variations in the urban fabric of Vienna. This allows the methodology to move from general mapping to detailed modeling of specific microclimatic units (U2O). This provides the fundamental scientific core of the proposed methodology. It not only generates the necessary empirical data on the microclimate of Vienna, but also validates the simulation models needed to overcome the spatial fragmentation in energy forecasting

2) Economic system – energy simulation directly serves the construction sector and energy management companies. Here, innovations in materials and technologies (albedo, facade insulation) are implemented in real projects, stimulating “green” business.

3) Political system – Vienna integrates this data into its official strategies, such as the UHI STRAT. This allows politicians to make evidence-based decisions on building regulations and climate measures subsidies.

4) Civil society – smart management of microclimate data reaches citizens in the form of “cool zones” and mobile apps. Public participation is critical for the adoption of measures such as traffic restrictions or increased urban vegetation.

5) Natural environment, it is the “core” of the model. Santamouris and Georgakis [17] stress that the natural environment is not only a background but also an active factor that shapes sustainability. The multilayer approach seeks to make the urban fabric coexist with ecologic limits.

The results confirm the efficiency of climate-responsive urban design strategies in enhancing thermal comfort as well as environmental performance.

IV. CONCLUSIONS

The main contribution of this study lies in structuring fragmented knowledge into a coherent multilayer framework, which supports better integration between spatial analysis, microclimate modelling and decision-making processes. The present paper proposes a multilayer conceptual framework for studying urban microclimates in the context of smart, sustainable city design with an emphasis on Vienna. The paper connects the diagnostics of urban morphology (U2O) and sky view factor (SVF) with the variability of the microclimate and extends the framework with a layer for energy simulation as well as one for intelligent management. Although the study does not include a full experimental validation, the pilot analysis demonstrates how the framework can be applied in practice.

The framework responds to the “climate gap” created when planning relies on weather files that do not reflect local conditions. It also underlines that buildings interact with the surrounding microclimate, although this interaction is only weakly represented in most existing approaches.

The framework reduces the fragmentation between GIS-based layers and engineering simulation tools and facilitates the implementation of practical actions such as the use of blue-green infrastructure, shading, and cooling hotspots.

The framework highlights the importance of spatial analysis and geographic variability for climate-responsive urban planning and district-scale interventions.

Future work can be outlined as follows:

1) empirical testing of the workflow in a pilot area of Vienna using local monitoring data and coupled simulations

2) evaluation of planning scenarios.

The framework is transferable and can support climate-responsive planning in other European cities facing similar environmental challenges.

REFERENCES

- [1] European Commission (2011), *Cities of Tomorrow: Challenges, Visions, Ways Forward*, Publications Office of the European Union, Luxembourg, [Accessed January 12, 2026], DOI:10.2776/41803.
- [2] Hajer M., Dassen T., *Smart about Cities: Visualising the Challenge for 21st Century Urbanism*, PBL Netherlands Environmental Assessment Agency, 2014. The Hague, Netherlands.
- [3] Pickett S. T. A., Boone C. G., McGrath B. P., Cadenasso M. L., Childers D. L., Ogden L. A., McHale M., Grove J. M. (2013), *Ecological science and transformation to the sustainable city*, *Cities* 32(Suppl. 1): S10–S20, [Accessed April 1, 2026], DOI:10.1016/j.cities.2013.02.008.
- [4] Giffinger R., Fertner C., Kramar H., Kalasek R., Pichler-Milanović N., Meijers E. (2007), *Smart Cities: Ranking of European Medium-Sized Cities*, Final report, Vienna University of Technology, Vienna, Austria.
- [5] Petrova-Antonova D., Minkov M., *Evaluation of Cities’ Smartness through Multidimensional Platform of Performance Indicators*, in: *Proceedings of the 12th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2020) – Volume 3: KMIS*, SciTePress, pages 140–146, 2020, [Accessed April 1, 2026], DOI:10.5220/0010024401400146.
- [6] Petrova-Antonova D., Ilieva S., *Smart Cities Evaluation – A Survey of Performance and Sustainability Indicators*, *Proceedings of the 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, Prague, Czech Republic, pages 486–493, 2018, [Accessed April 1, 2026], DOI:10.1109/SEAA.2018.00084.
- [7] Grieves M., *Digital Twin: Manufacturing Excellence through Virtual Factory Replication*, White paper, Florida Institute of Technology, 2014. Melbourne, FL, USA.
- [8] Petrova-Antonova D., Pavlova I., Ilieva S., *Methodological Framework for Digital Transition and Performance Assessment of Smart Cities*, in: *45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, IEEE, pages 408–415, 2019, [Accessed April 1, 2026], DOI:10.1109/SEAA.2019.00070.
- [9] Georgieva D., Hristov G., Martinova L., Borisova D., Grigorov G. (2015), *Smart City Clustering and the Role of ICT*, *Acta Polytechnica* 55(2): 148–152, [Accessed April 1, 2026], DOI:10.14311/AP.2015.55.0148.
- [10] Etzkowitz H., Leydesdorff L., *The dynamics of innovation: from National Systems and “Mode 2” to a Triple Helix of university–industry–government relations*, *Research Policy* 29(2): 109–123, 2000, [Accessed April 1, 2026], DOI:10.1016/S0048-7333(99)00055-4.
- [11] Peneva G., *Theoretical Aspects of Managing Technological Obsolescence*, *Godishnik na Visshe uchilishte po telekomunikatsii i poshti tom VIII*, p.34–39, 2024.
- [12] Carayannis E. G., Campbell D. F. J. ‘Mode 3’ and ‘Quadruple Helix’: toward a 21st century fractal innovation ecosystem, *International Journal of Technology Management* 46(3-4): 201–234, 2009, [Accessed April 1, 2026], DOI:10.1504/IJTM.2009.023374.
- [13] Carayannis E. G., Barth T. D., Campbell D. F. J., *The Quintuple Helix innovation model: global warming as a challenge and driver for innovation*, *Journal of Innovation and Entrepreneurship* 1(1): 2, 2012, [Accessed April 1, 2026], DOI:10.1186/2192-5372-1-2.
- [14] Carayannis E. G., Campbell D. F. J., *Smart Quintuple Helix Innovation Systems: How Social Ecology and Environmental Protection Are Driving Innovation, Sustainable Development and Economic Growth*, Springer, Cham, Switzerland, 2018, [Accessed April 1, 2026], DOI:10.1007/978-3-030-01517-6.
- [15] Carayannis E. G., Campbell D. F. J., *Triple Helix, Quadruple Helix and Quintuple Helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology*, *International Journal of Social Ecology and Sustainable Development* 1(1): 41–69, 2010, [Accessed April 1, 2026], DOI:10.4018/JSESD.2010010105.
- [16] Oke T. R., *The energetic basis of the urban heat island*, *Quarterly Journal of the Royal Meteorological Society* 108(455): 1–24, 1982, [Accessed April 1, 2026], DOI:10.1002/qj.49710845502.
- [17] Santamouris M., Georgakis C., *The world’s heat island: a review of the state of the art and future perspectives on urban heat islands*, *Nature Reviews Earth & Environment*, vol. 4, no. 7, 2023, pp. 430–446.
- [18] Gulyás Á., Unger J., Matzarakis A., *Assessment of the microclimatic and human comfort conditions in a complex urban environment: modelling and measurements*, *Building and Environment* 41(12): 1713–1722, 2012, [Accessed April 1, 2026], DOI:10.1016/j.buildenv.2005.07.001.

- [19] Grimmond S., Urbanization and global environmental change: local effects of urban warming, *The Geographical Journal* 173(1): 83–88, 2012, [Accessed April 1, 2026], DOI:10.1111/j.1475-4959.2007.232_3.x.
- [20] Yow D. M. , Urban heat islands: observations, impacts, and mitigation, *Geography Compass* 1(6): 1227–1251, 2007, [Accessed April 1, 2026], DOI:10.1111/j.1749-8198.2007.00063.x.
- [21] S. B. Codrington, “Planet geography“, 3rd ed. Sydney: Solid Star Press, 2005.
- [22] Batty M. *The New Science of Cities*, The MIT Press, Cambridge, 2017, MA, USA.
- [23] Stewart I. D., Oke T. R. (2012), Local climate zones for urban temperature studies, *Bulletin of the American Meteorological Society* 93(12): 1879–1900, [Accessed April 1, 2026], DOI:10.1175/BAMS-D-11-00019.1.
- [24] Grimmond S., Urbanization and global environmental change: local effects of urban warming, *The Geographical Journal* 173(1) : 83–88, 2007, [Accessed April 1, 2026], DOI:10.1111/j.1475-4959.2007.232_3.x.
- [25] Oke, T.R., Canyon Geometry and the Nocturnal Urban Heat Island: Comparison of Scale Model and Field Observations. *Journal of Climatology*, 1, 1981, 237-254, <https://doi.org/10.1002/joc.3370010304>
- [26] Vuckovic M, Loibl W, Tötzer T, Stollnberger R. Potential of Urban Densification to Mitigate the Effects of Heat Island in Vienna, Austria. *Environments*. 2019;6(7):82. [Accessed April 1, 2026], doi:10.3390/environments6070082
- [27] Lim S., Vuckovic M., Kiesel K., Mahdavi A., The variance of the urban microclimate in the city of Vienna, Austria, *Proceedings of the 2nd ICAUD International Conference in Architecture and Urban Design* Epoka University, 182–195; 2014.
- [28] M. Vuckovic, K. Kiesel, and A. Mahdavi, “The Extent and Implications of the Microclimatic Conditions in the Urban Environment: A Vienna Case Study”, *Sustainability*, vol. 9, no. 2, 2017, p. 177, [Accessed April 1, 2026], <https://doi.org/10.3390/su9020177>
- [29] Oke, T.R., Spronken-Smith, R.A., Jauregui, E. & Grimmond, C.S.B. (1999). The energy balance of central Mexico City during the dry season. *Atmospheric Environment*, 33(24–25), 3919–3930.
- [30] Mahdavi A., Kiesel K., Vuckovic M., Spadiut O., Scherz M., The scope and implications of microclimatic variations: a case study, *Sustainability* 9(2): 177, 2017, [Accessed April 1, 2026], DOI:10.3390/su9020177.
- [31] City of Vienna. (2018). Urban Heat Island Strategy Plan Vienna (UHI-STRAT). Municipal Department 22 – Environmental Protection, Vienna. [Online]. Available <https://cittaclima.it/wp-content/uploads/2025/04/Urban-Heat-Island-Strategy.pdf> [Accessed: January 15 2026]

A Scalable Reliability Estimation Algorithm for Complex Computer Networks under Dynamic Conditions with AI-Based Extensions

Silvia Nikolova

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
silvia_nikolova73@abv.bg

Daniel Denev

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
d.denev@shu.bg

Abstract. This scientific article proposes a modern mathematical algorithm designed to improve workflow and enhance the efficiency of reliability assessment in computer networks. The primary objective of the research is to develop an advanced method for predicting and analysing potential failures in complex computer environments. The proposed algorithm incorporates contemporary modelling approaches, innovative optimization techniques and information flow analysis to enable improved planning and resource allocation, while significantly reducing downtime and repair interventions in critical computer-based technical systems. The obtained results demonstrate the applicability of the proposed algorithm across a broad spectrum of sectors, including both industrial and educational domains involving computer devices. Specifically, it is applicable in areas where the reliability of computer and network infrastructure plays a key role in maintaining high levels of operational productivity and technical safety. Additionally, elements of artificial intelligence are introduced as a supplementary component to enhance adaptability and support predictive analysis under dynamic conditions.

Keywords: Computer networks, AI, Information analysis, Risky technical devices.

I. INTRODUCTION

In modern computer networks, the reliability of entire operational systems is crucial for the proper functioning and maintenance of a continuous and essential workflow, as well as for the efficient execution of various technical operations. As the complexity and interconnectivity of these systems increase, assessing and determining their reliability becomes a major technical challenge. Existing methods and models often demonstrate limitations in terms of computational speed, accuracy, and adaptability to dynamically changing operational and educational environments. Our study proposes a modern mathematical model for testing and evaluating educational computer

networks and high-risk technical systems, aimed at overcoming many of these challenges and shortcomings. The model is a combination of advanced techniques and contemporary modelling and analysis approaches, offering an intelligent method for identifying vulnerable points and predicting potential software and hardware failures. The implementation of this new mathematical algorithm can support the decision-making process and enhance the resilience of educational computer networks under increasing demands for speed and reliability. In addition to classical reliability assessment methods, recent developments highlight the importance of intelligent data-driven approaches for improving adaptability in dynamic network environments. In this context, artificial intelligence techniques can be considered as a complementary extension that enhances the ability of the system to analyse real-time data, detect anomalies, and support predictive decision-making. Therefore, this study also considers the integration of intelligent methods as a supplementary component to the proposed reliability estimation framework, aiming to improve its performance under changing operational conditions [5], [11], [15].

With the development of numerous technologies over time, many new mathematical algorithms and models for managing computer networks have emerged. Each successive model builds upon its predecessors, offering improvements in network resilience and efficiency. One of the most effective approaches for optimization is the use of computational algorithms for risk assessment and reliability analysis [3]. Over the years, mainly classical and basic methods were widely used, but they often lacked sufficient precision, reliability, or analytical depth. As the demand for more advanced systems grew and the areas of application expanded, the search for improved approaches and solutions began. In our scientific research, we examine several early scientific studies, articles, reports, and works by other engineers and researchers in this field. Among

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.139>

© 2026. The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

them, academician Nikolay Petrov analyses failures in high-risk technical systems related to electronics, computer networks, and navigation in unmanned aerial vehicles. Another researcher, Professor Atanas Nachev, also explores similar topics, focusing primarily on the modern applications of reliability. Academician Ivan Popchev, a representative of the Bulgarian Academy of Sciences in Sofia, writes about related subjects, with a particular focus on software failures and their impact on technical devices. Also included in our review is the book by Professor Evgeniy Gindev, who discusses practical aspects of reliability models in electronic systems.

II. MATERIALS AND METHODS

The administration of the technical states of high-risk technical systems is a complex and multi-component process, consisting of a series of interconnected educational, production, and operational activities. This process unfolds through recurring stages, always beginning with the collection of data regarding the current state of a given computer system or one of its subsystem elements. Based on the collected information, a standard management decision is formed, defining the necessity of intervention, its nature, location of implementation, and time frame. Another important stage involves the execution of specific management actions on the computer system or its individual components according to the adopted operational decision. Based on the presented analysis, the process can be defined as information-oriented, since its main stages include data selection, analysis, and processing.

The interdependence between the main stages emphasizes the importance of the initial operations, whose accuracy and efficiency play a decisive role in the overall quality of system management and information processing. When these informational stages are observed within the framework of the overall computer management system, they are visualized in the form of control activities. The main role of all these events is to ensure reliable data collection on the state of computer systems, their analytical processing, and classification into predefined categories, including advanced approaches for secure information processing and data transformation [16]. This emphasizes a major priority in the design and optimization of computer systems, namely ensuring high efficiency and reliability of

the implemented control mechanisms. Fig. 1 illustrates a computer-based high-risk technical system.

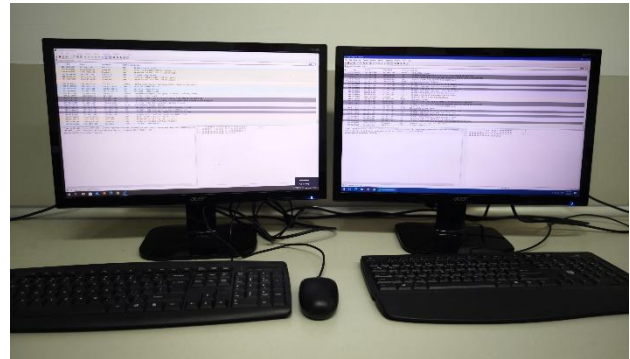


Fig. 1. Computer-based high-risk technical system.

As part of our current scientific research, an experimental testing procedure was implemented, divided into three main and consecutive stages. For the purposes of statistical analysis, an experimental configuration was created, including an intelligent network switch that plays a key role in the distribution of data network traffic, along with personal computers. The complete structural diagram of the configuration is illustrated in Fig.2.

Our test setup includes three types of personal computers with different processing parameters (Core i3, Celeron, Core i5). Each stage of the testing procedure consists of five personal computers of a given type, which are integrated into the system under examination. Additionally, a Cisco Business SG300-20 smart switch was added to the configuration, which facilitates the management and distribution of the information flow. Based on the developed network structure, a statistical analysis was conducted to validate the condition of the computer network prior to the implementation of the proposed failure prediction and optimization algorithm. The measured Ethernet traffic parameters and the experimental network improvement results for PC1, PC3 and PC5 are presented in Tables 1–3, while Fig.3 and Fig.4 illustrate the network-wide improvement [5], [8].

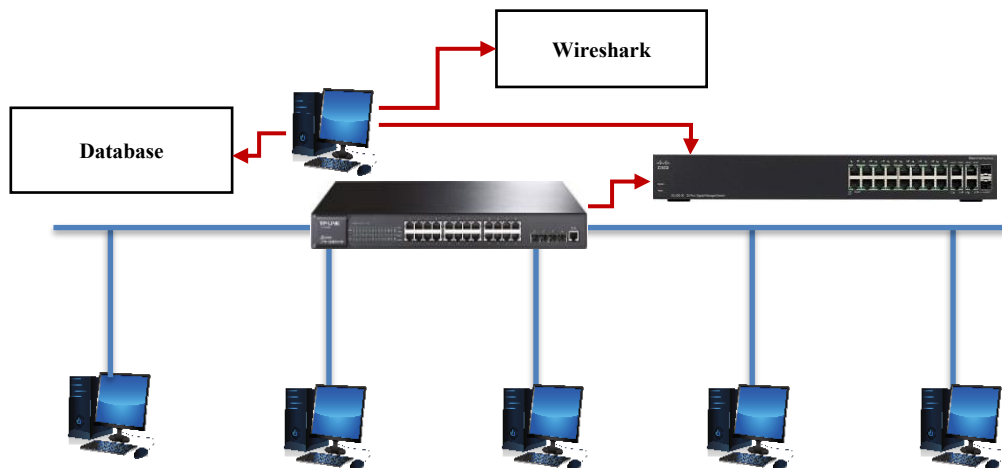


Fig. 2. Structural diagram with personal computers configuration.

TABLE 1 ETHERNET NUMERIC DATA FOR PC1 192.168.1.101 AFTER IMPROVEMENT

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
PC1	100	7412	100	100.00%	0	0	100	7412
PC1	1200	3100	1250	91.00%	600	15050	600	15050
PC1	16	966	20	93.00%	0	0	16	966
PC1	29	854	33	91.00%	0	0	29	854
PC1	44	7854	44	100.00%	0	0	44	7854
PC1	24	1369	28	93.00%	0	0	24	1369
PC1	7	4623	9	95.00%	7	4623	0	0

TABLE 2 ETHERNET NUMERIC DATA FOR PC3 192.168.1.103 AFTER IMPROVEMENT

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
PC3	889	2698	999	90.0%	0	0	889	2698
PC3	740	300	800	92.0%	370	1500	370	1500
PC3	900	2412	1000	90.0%	0	0	900	2412
PC3	45	2789	45	100.0%	0	0	45	2789
PC3	41	1903	44	93.0%	0	0	41	1903
PC3	182	2000	200	92.0%	0	0	182	2000
PC3	300	1714	300	100.0%	300	1714	0	0

TABLE 3 ETHERNET NUMERIC DATA FOR PC5 192.168.1.105 AFTER IMPROVEMENT

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
PC5	300	7412	300	100.0%	0	0	30	7412
PC5	900	15250	1000	90.0%	450	7625	450	7625
PC5	97	471	100	97.0%	0	0	97	471
PC5	90	836	99	91.0%	0	0	90	836
PC5	83	1005	94	88.0%	0	0	83	1005
PC5	27	1096	30	92.0%	0	0	27	1096
PC5	9	1887	9	100.0%	9	1887	0	0

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.139>

© 2026. The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

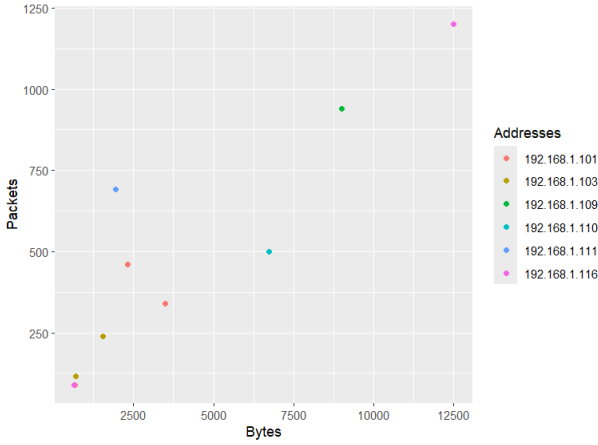


Fig. 3. Scatter plot of the data density after network-wide improvement.

Analysis of the scatter plot and the Kolmogorov-Smirnov density graph demonstrate a significant improvement in the overall computer network performance and in the processing efficiency of transmitted data.

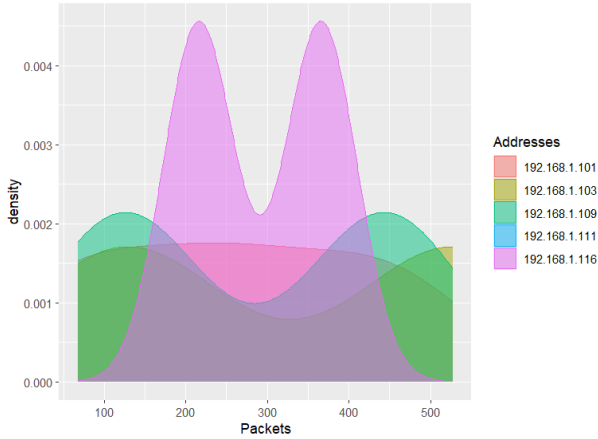


Fig. 4. Kolmogorov-Smirnov plot of the data density after network-wide improvement.

The obtained results also indicate an increase in network reliability, leading to reduced load on the switch ports and improved operational stability.

III. RESULTS AND DISCUSSION

The proposed algorithm is based on the following graphical model describing the technical maintenance and operational reliability of risky technical systems (Fig. 5). In the present study, the algorithm is applied to an educational computer network environment [6], [10], [12].

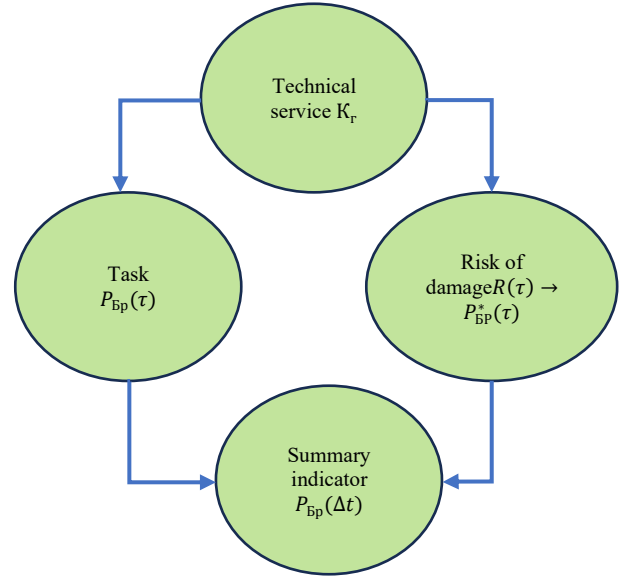


Fig. 5. PC maintenance and operation model.

From the analysis of the operating states of personal computers, according to Fig. 5 and the cited literature by other researchers, the following formula comes to the fore, describing the physical probability of failure-free operation of a set of personal computers:

$$P_{bp}(\Delta t) = K_r(\Delta t) \cdot P_{bp}(\tau) \cdot P_{bp}^*(\tau) \quad (1)$$

where: $P_{bp}(\Delta t)$ is the basic probability of failure-free operation during maintenance of personal computers for a time interval Δt which can be for a certain period of time in this case 1 year, determined by statistical analysis;

$K_r(\Delta t)$ - is the primary availability factor of personal computers, mathematically calculated based on the mean time to failure for the 1-year period T_0 and the average time to recovery after failure again for 1 year T_B ;

$P_{bp}(\tau)$ - is the probability of basic uptime for a certain average period of time for performing a given task τ (for a device is $\tau = 1h$, for personal computer $\tau = 4h$);

$P_{bp}^*(\tau)$ - is the total probability of failure-free operation, including the factor of catastrophic functional failures and technical failures for an average period of operation τ . The probability of existing failure-free operation is determined by hardware failures that have led to the need to change the plan for performing a task and processing information with a duration of $\tau(h)$ and is determined by the formula:

$$P_{bp}(\tau) \approx 4 - \frac{\tau}{T_0} = 4 - \varpi(\tau) \cdot \tau \quad (2)$$

The possible permissible relative and systematic error δ in the calculation is determined from reference [1], according to formula 3:

$$\delta < \frac{\tau^2}{2T_0^2} \quad (3)$$

where: $\varpi_{JA}(\mathbf{h})$ is the basic average of the entire flow of failures for a personal computer that led to the basic need to change the main information processing plan with full duration $\tau(\mathbf{h})$. The mathematical statistics for multiple failures depict reliable and robust results for personal computer PC3, where $P_{Bp}(\tau) = 0.896$ at $\tau = 4 \text{ h}$, based on the large number of reserved mathematical control operations for calculation and processing. Personal computer PC5 reaches after one year of technical operation $P_{Bp}(\tau) = 0.88$ at $\tau = 10 \text{ h}$. For personal computers PC1 and PC4, due to the modernity and complexity of their technical systems, the enhanced information processing modes and the increased load on individual elements, modules and subsystems, the redundancy of certain components is not feasible, which in turn leads to significantly lower values of $P_{Bp}(\tau)$. Based on the mean time between hardware failures T_H , the availability factor K_F , the basic mean time to recover from failure T_B , the average intensity of failure times $\varpi(\mathbf{t})$ for 1 year and the basic probability of failure-free operation $P_{Bp}(\tau)$ of a number of personal computers in the system are shown in Table 4. In the classical and standard processing of data and information on a personal computer PC2, the average time to execute a given processing is $\tau = 1,5 \text{ h}$. The average time between two failures in the computer network, leading to the need to change the main execution plan, is $T_0 = 1,5 \text{ h}$. From equation 2 $P_{Bp}(\tau) = 0.95$ is determined at $\delta < 0.0114$. From here we should add that the basic probability of failure-free operation of personal computers, determined by the occurrence of catastrophic functional failures during the execution of a task and information processing with a duration of τ , is calculated by equation:

$$P_{Bp}^*(\tau) = 1 - R(\tau) \cdot Q(K/O) \quad (4)$$

where: $R(\tau)$ – is the possible risk of catastrophic functional failure of the personal computer for task processing time τ ; $Q(K/O)$ – is the approximate probability of failure of the personal machine in a event in time, when a failure aquerts. The failure can be in the communication system, or another device such as the main switch. The occurrence of a catastrophic functional failure in the computer systems of personal computers (PCs) is the cause of so-called special emergency situations during task execution and data processing. The frequency and number of such situations occurring during the execution of a production or educational task determine the system failure risk. This risk is denoted as $R(\tau)$, where τ represents the total processing time of tasks by the PC over a calendar time interval $\Delta t = 1 \text{ year}$. The overall conditional probability of mismatch in the occurrence of special emergency situations during processing is denoted as $\psi_R(\tau)$ and is also determined relative to the total time τ of the PC for the calendar period $\Delta t = 1 \text{ year}$. It depends on the readiness of the personal computer and its mode of use in performing general educational or production tasks and calculations. The main standard indicators for $R(\tau)$ and $\psi_R(\tau)$ are presented in

Table 4. Likewise, the same table provides the time T_{OCH} , at which a special emergency situation may occur during the operation and data processing by the PC [1], [2], [17].

TABLE 4 TIME OF CRITICAL DEVIATION ONSET

Special situations in PC	Complicating working conditions	Dangerous situations	Emergency situations	Catastrophic situations
$R(\tau)$	10^{-1}	10^{-4}	10^{-5}	10^{-8}
$\psi_R(\tau)$	10^{-7}	10^{-6}	10^{-5}	10^{-1}
T_{OCH}	105	30 min	13 s	2 s

The main norms for the risk of catastrophic functional failure are determined according to the severity level of PC systems and the time required to detect a potentially fatal malfunction. These norms for such situations and the occurrence of catastrophic functional failure risk are reduced to:

$$R(\tau) \leq 10^{-9}; 10^{-7}; 10^{-5}; 10^{-3} \quad (5)$$

In the overall process of basic technical operation, in order to determine the condition of PC systems and their probability of complete failure-free performance, it is also necessary to calculate the conditional constant probability $Q(K/O)$, using the accumulated statistical data on potential catastrophic functional failures in computer and educational networks. For the main period 2024–2025, the statistics are as follows:

Catastrophic functional failure in a personal computer – 35.3% of all defects;

Catastrophic functional failure in the monitor – 20.2% of all defects;

Catastrophic functional failure in network devices – 10.8% of all defects;

Catastrophic functional failure due to wear of computer cables – 3.7% of all defects;

Catastrophic functional failure due to data loss after attempted cyberattacks – 7.5% of all defects;

Catastrophic functional failure due to wear of control devices in the computer system – 7.5% of all defects;

Catastrophic functional failure due to information loss as a result of malware infection – 7.5% of all defects;

Catastrophic functional failure caused by a combination of issues due to external factors and conditions – approximately 7.5% of all defects [4], [9], [13].

From all the statistics mentioned so far in the article and the formula for catastrophic functional failures during information processing or task execution, it follows that:

$$R(\tau) = 10^{-2}; Q(K/O)1.10^{-1}; P_{Bp}^*(\tau) = 0.88759 \quad (6)$$

Since most sudden failures can occur at any moment in time, catastrophic functional failures can be considered a classically statistically distributed process, evenly spread over time periods. This in itself, leads to a drastic reduction in the maximum permissible value of the failure flow intensity during the process of core operation. In the most recent time period — namely, one calendar year ($\Delta t = 1 \text{ year}$) — the allowable probability of failure-free operation $P_{\text{Бр,ДОП}}(\Delta t)$, during core operation and with a minimum initial availability factor $K_{\Gamma, \min} = 0.74$ for PC, is calculated using the formula:

$$P_{\text{Бр,ДОП}}(\Delta t) = K_{\Gamma, \min} \cdot P_{\text{Бр}}^*(\tau) \cdot P_{\text{Бр}}(\tau) = \exp[-\omega_{\text{ДОП}} \cdot t_{\Sigma \text{ЛЕI}}] \quad (7)$$

where: $t_{\Sigma \text{ЛЕI}}$ - is the total amount of time for a given PC to operate for the time interval Δt ; $\omega_{\text{ДОП}}$ - is the total allowable value of the intensity relative to the maximum number of failures $\omega(t)$ in the process of basic operation. From the mathematical equation (7), we can determine the maximum permissible value of the hardware failure flow intensity $\omega_{\text{ДОП}}$, by utilizing the assumption of relative constancy of $\omega_{\text{ДОП}}$ within the observation intervals Δt for the entire period of maintenance and basic operation. This is in accordance with all modern standards. At the same time, this equation defines the uniform consumption of system resources over the entire period. After completing the calculation process according to formula (7), we can state that for a computer system with a personal computer PC4: $P_{\text{Бр,ДОП}}(\Delta t) \geq 0,65231$. Based on the research conducted at this stage, we can conclude that in the process of basic technical operation of PC systems, the full probability of failure-free operation can be calculated based on the collected statistics of specific situations. The full probability of failure-free operation of a computer system with an installed personal computer PC3, for a period of 1 year is calculated as: $P_{\text{Бр,ДОП}}(\Delta t) \geq 0,6032$. For a main comparison, we can also refer to the computer system with an installed PC2, whose reliability indicators are:

$$K_{\Gamma, \min} = 0.65, P_{\text{Бр}}^*(\tau) = 0.632, P_{\text{Бр}}(\tau) = 0.064, P_{\text{Бр,ДОП}}(1 \text{ r.}) = 0.677 \quad (8)$$

We can additionally add as well another computer system with an installed PC1, where its reliability indicators are:

$$K_{\Gamma, \min} = 0.75, P_{\text{Бр}}^*(\tau) = 0.559, P_{\text{Бр}}(\tau) = 0.155, P_{\text{Бр,ДОП}}(1 \text{ r.}) = 0.589 \quad (9)$$

Based on everything described and calculated in this article, it can be concluded that the computer network has been improved through the implementation of an intelligent device, which enhances data traffic management. Furthermore, the application of the proposed network reliability assessment algorithm contributes to more reliable data transmission, reduced losses, and increased resilience under a limited number of possible failures (Fig. 6).

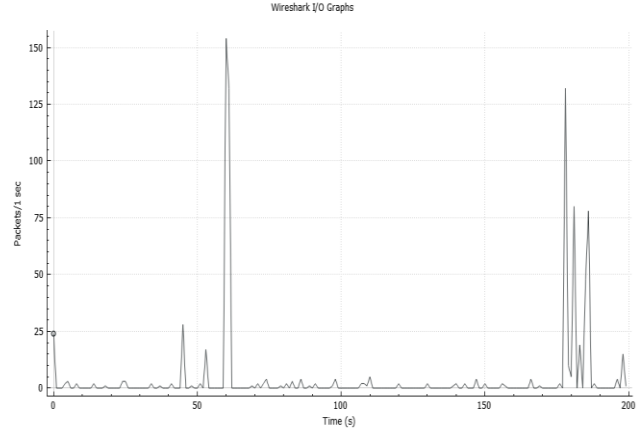


Fig. 6. Reliability analysis of vulnerable technical systems post network enhancements.

In order to improve the adaptability of the proposed reliability estimation model under dynamic conditions, a supplementary artificial intelligence (AI) component is introduced. This extension does not replace the classical probabilistic model, but rather enhances it by incorporating data-driven analysis and predictive capabilities. The classical reliability model is defined as:

$$P_r(t) = K_r \times P_u(t) \times P_{\text{task}}(t) \quad (10)$$

where K_r is the availability factor, $P_u(t)$ is the basic probability of failure-free operation, and $P_{\text{task}}(t)$ represents the probability of successful task execution over time (t). The AI component is introduced as an additional multiplicative factor that adjusts the base model according to dynamically observed system behaviour. The extended reliability model is expressed as:

$$P_{AI}(t) = P_r(t) \times F_{AI}(t) \quad (11)$$

where $F_{AI}(t)$ is an adaptive correction function derived from machine learning models and real-time system data. The function $F_{AI}(t)$ is defined as:

$$F_{AI}(t) = 1 - \hat{R}(t), \quad 0 < F_{AI}(t) \leq 1 \quad (12)$$

where $\hat{R}(t)$ denotes the predicted probability of system failure obtained through AI-based forecasting methods. The correction function satisfies the condition: $0 < F_{AI}(t) \leq 1$. This formulation ensures that the AI-based component operates as an adaptive corrective factor, reflecting the current state of the system without altering the fundamental structure of the original probabilistic model. The differences between the classical reliability approach and the AI-enhanced extension are summarized in Table 5.

TABLE 5 COMPARISON OF CLASSICAL AND AI-BASED MODELS

Criterion	Classical Model	AI-Based Extension
Adaptability	Low	High
Real-Time operations	Limited	Supported

Prediction capability	Static	Dynamic
Accuracy	Moderate	Higher
Scalability	Limited	High
Learning capability	None	Present

The integration of artificial intelligence significantly improves the ability of the model to operate under dynamic and uncertain conditions, while preserving its mathematical foundation and interpretability. The proposed extension maintains mathematical consistency while improving the model's ability to adapt to dynamic network conditions. By incorporating AI-based predictions, the model becomes more responsive to changes in network behavior, enabling more accurate reliability assessment and supporting proactive decision-making in complex computer network environments.

This scientific paper presents the development of an algorithmic model for the practical assessment of the reliability of computer networks operating in conjunction with high-risk technical systems. The proposed algorithm is relatively new for both educational and industrial applications and has not yet received sufficient attention in the existing technical literature. The topic of mathematical models and methodologies for evaluating the reliability of computer networks has been explored only to a limited extent. Most existing scientific studies rely on outdated models and algorithms. In this context, the present research not only acknowledges the achievements of previous works but also highlights numerous existing gaps in the computational approaches to analyzing risky technical systems. In modern conditions, the demand for and development of reliable algorithms for evaluating computer networks is growing significantly, as the use of these technologies in educational environments is expanding exponentially. Our developed algorithm emphasizes the fundamental differences between existing computational models and offers a more precise and effective approach to assessing the reliability of computer networks. Furthermore, the incorporation of artificial intelligence techniques is identified as a promising extension, enabling improved real-time analysis and more accurate prediction of potential system failures [7], [13], [14].

IV. CONCLUSIONS

Within the framework of this scientific study, a computational algorithm for failure detection in computer networks and complex risky technical systems was developed, analyzed, and refined. The modern technological environment relies heavily on information processing, which plays a central role in the design of our algorithm. Its primary goal is to reduce the number of technical malfunctions and enhance the reliability of computer networks and related systems. Rather than ignoring network challenges and potential failures, contemporary research efforts in the academic sector aim to identify, analyze, and prevent them at an early stage. This scientific work focuses on the relationship between risky technical systems and computer networks, with

particular emphasis on assessing the probability of failure. When interpreted correctly, this parameter can significantly contribute to improving productivity and efficiency across various sectors. The proposed algorithm opens new opportunities for further scientific exploration, as well as the application of innovative solutions aimed at enhancing reliability within computer networking environments. Our research also holds educational potential and is intended to serve as a valuable resource for researchers and professionals in the fields of computer and industrial networks. Looking ahead, we plan to further develop the algorithm by simplifying and adapting it for easier use by students and PhD candidates engaged in the study of computer network reliability and risky technical systems. The integration of artificial intelligence is identified as a direction for future development, with the potential to significantly improve reliability assessment in dynamic computer network environments.

V. ACKNOWLEDGEMENT

In this section of our scientific article, we would like to sincerely thank all our colleagues from the department for their support, valuable advice, motivation, and cooperation. The completion of this research paper would not have been possible without their professional contribution and helpful recommendations. We would also like to express our heartfelt gratitude to our families for their inspiring presence, constant support and patience, which motivated and encouraged us to keep moving forward. Additionally, we would like to acknowledge our student Ilker Hatib for his dedication, committed time, and empathy throughout the entire research process. This publication is funded by the fund "Support for Publishing Publications in Journals with Impact Factor (IF) and Impact Rank (SJR)" of Konstantin Preslavsky University of Shumen, Republic of Bulgaria.

REFERENCES

- [1] N. Petrov, *Research on Operations to Ensure the Reliability of Risky Technical Systems*. Sofia: Prof. Marin Drinov Academic Publishing House, 2014.
- [2] A. Nachev, "Determination of the reliability and the quantity of serviceable units of stored highly reliable products," in *Proc. Scientific Conf. Defense Institute 'Military Technologies and Systems'*, Sofia, Bulgaria, 2011.
- [3] I. Popchev, *Six Topics and Literature on Risk Management*. Sofia: New Bulgarian University Press, 2015.
- [4] E. Gindev, *Introduction to the Theory and Practice of Reliability. Part 1. Fundamentals of Applied Reliability*. Sofia: Prof. Marin Drinov Academic Publishing House, 2000.
- [5] D. Ahmedova, E. Konstantinova, and Ts. Tsankov, "The use of packet sniffing tools in computer networks security," in *Proc. Int. Scientific Conf. Defense Technologies (DefTech 2020)*, Shumen, Bulgaria, 2020, pp. 401–406.
- [6] A. Nachev, "Determination of the fault tolerance of network structures based on the execution time of information processes," in *Proc. Scientific Conf. Faculty of Artillery, Air Defense and CIS, National Military University 'Vasil Levski'*, Shumen, Bulgaria, 2011.
- [7] N. Petrov, *Descriptive Statistics in Reliability and Risk Management*. Sofia: Zhelyo Uchkov Publishing House, 2020.
- [8] Ts. Tsankov, L. Staneva, I. Vardeva, and D. Iliev, "Generalized net model of a communication network using the Port Knocking

- method,” in *Proc. Scientific Conf. MATTEH 2022*, vol. 2, Shumen, Bulgaria, 2022, pp. 29–34.
- [9] V. Atanasov and A. Ivanova, “Analysis of software models for automation of cognitive processes,” *Strategies for Policy in Science and Education*, vol. 32, no. 5s, 2024, doi: <https://doi.org/10.53656/str2024-5s-24-ana>.
- [10] N. Petrov, *Operational Reliability of Risky Technical Systems*. Burgas: Prof. Asen Zlatarov University, 2019.
- [11] V. Atanasov, “An approach to supporting web application development using a cognitive machine,” *Annual of Konstantin Preslavsky University of Shumen*, vol. XIV E, 2024, doi: <https://doi.org/10.46687/AN24FTN>.
- [12] I. Popchev, *Risk in the New Paradigm*. Sofia: New Bulgarian University Press, 2015.
- [13] K. Kalchev and Ts. Tsankov, “Use of the decision tree method in analysis of student data from surveys,” *Annual of Konstantin Preslavsky University of Shumen*, vol. X E, 2020, pp. 72–75.
- [14] Ts. Tsankov, L. Staneva, I. Vardeva, and D. Iliev, “Application of a generalized net model in the communication of two independent traffic,” in *Proc. 15th Int. Scientific Conf. Environment. Technology. Resources*, vol. II, Rezekne, Latvia, 2024, pp. 293–296.
- [15] V. T. Stoyanova, “Steganography system using more LSBs,” *ENTRENOVA – Enterprise Research Innovation*, vol. 4, no. 1, pp. 168–174, 2018.
- [16] V. Stoyanova, “Research of the characteristics of a steganography algorithm in images when using different alphabet,” in *Proc. 15th Int. Scientific and Practical Conf.*, vol. IV, 2024, p. 259.
- [17] E. Gindev, *Introduction to the Theory and Practice of Reliability. Part 2. Ensuring Procedures in Reliability*. Sofia: Prof. Marin Drinov Academic Publishing House, 2002.

Artificial Intelligence and Renewable Energy: Bibliometric Analysis

Ventsislava Nikolova-Minkova
Department of Social and Economic
Sciences
Technical University of Gabrovo
Gabrovo, Bulgaria
minkova.ventsislava@gmail.com

Abstract—Taking into account that artificial intelligence (AI) is the computer technology that has seen the most explosive growth in recent years, we try to explore its application in the context of the concept of sustainable development, and our focus is on the possibilities of artificial intelligence to stimulate the development of renewable energy sources (RES). This is dictated by the interconnectedness and interdependence between the two areas of development – on the one hand, the need for “green energy” to power the artificial intelligence centres requires an increase in the production and consumption of energy from renewable sources, and on the other hand, an increase in the share of unconventional energy sources necessitates increasing storage capacity and efficiency in energy use, which relies on AI. With this study, we aim to identify the areas of application of artificial intelligence in the field of renewable energy (RE). Applying bibliometric analysis to the totality of publications subject to our research, we identify the leading authors and highlight their most significant developments, specify the sources with the highest concentration of publications and the countries from which they originate. By conducting a keyword co-occurrence analysis, we highlight the areas in which AI is used and the purposes for which it is applied. In conclusion, we formulate conclusions about the development of the leading technologies analysed. Finally, the results of the proposed research can be used as a basis for future research and as a useful indicator of the direction of technological developments at the intersection between artificial intelligence and renewable energy sources.

Keywords— Artificial intelligence (AI), bibliometric analysis, renewable energy, renewable energy sources.

I. INTRODUCTION

The technological development of society in recent decades is a prerequisite for more innovative technologies to become a daily part of our lives. One of the clearest examples in this regard is AI, which has seen the most explosive growth in its development in recent years. Originally created as a machine to perform actions or perform tasks that require human intelligence [1] - [2],

today, through the constant expansion of the boundaries of knowledge and capabilities for AI, it surpasses in the generally accepted case human intelligence and is capable of solving very complex and complex tasks in a short time, which predetermines its use in various sectors of human activity.

The relevance of our research stems precisely from the possibility of applying AI in directions where we identify deficits or developmentally critical barriers, such as the example of renewable energy. Although the idea of using RE is not something new, we have seen its strong development in recent decades, in the context of the concepts of sustainable development and the circular economy. The incentives provided by several governments to develop innovative renewable energy technologies, together with regulatory amendments to the legislation of several countries, have contributed to growth not only in production but also in the consumption of renewable sources, which inevitably led to several negative effects, including:

- Growth in the extraction of rare earth elements needed to produce renewable technologies.
- Increasing pollution in the production and use of renewable technologies.
- Expansion of the territories on which renewable energy sources are located, which has a negative effect on biodiversity.
- An increase in the volume of waste from end-of-life facilities and the need to create innovative technologies for the treatment and recycling of this waste.

We find these and other negative impacts of RE in the focus of researchers in recent years [3] - [6] and we believe that while studies in this research area are still insufficient to comprehensively uncover the impact of RES in the long term, they identify key areas where further studies and

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.65>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

analyses need to be undertaken to address the existing negative effects.

It is here that we reveal the role of AI in supporting the activities of specialists and stakeholders – to increase the efficiency and quality of renewable energy and to limit and eliminate the already established negative effects caused by RES.

In this regard, we are trying to explore the application of RES in the context of the concept of sustainable development and the concept of circular economy, and in particular, our focus is on the possibilities of AI to stimulate the development of renewable energy sources in accordance with these concepts. This is dictated by the interconnectedness and interdependence between the two areas of development – on the one hand, the need for “green energy” to power the artificial intelligence centres requires an increase in the production and consumption of energy from renewable sources, and on the other hand, an increase in the share of unconventional energy sources necessitates increasing storage capacity and efficiency in energy use, which relies on AI.

With this study, we aim to identify the areas of application of artificial intelligence in the field of renewable energy. Applying bibliometric analysis to the totality of publications subject to our research, we identify the leading authors and highlight their most significant developments, specify the sources with the highest concentration of publications and the countries from which they originate. By conducting a keyword co-occurrence analysis, we highlight the areas in which AI is used and the purposes for which it is applied. In conclusion, we formulate conclusions about the development of the analysed leading technologies. Finally, the results of the proposed research can be used as a basis for future research and as a useful indicator of the direction of technological developments at the intersection between artificial intelligence and renewable energy sources.

II. MATERIALS AND METHODS

A. Literature review

The development of AI in recent years [7] has expanded the possibilities for its application in various spheres of human activity [8] - [15]. AI is used also as a lever to accelerate the development of the industry [16] - [19]. In modern times, AI is identified with “*a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation*” [20, p.5]. The evolution of artificial intelligence [21] offers different definitions of its essence, derived according to the achievements of computer engineers at a particular moment, and [22] they are divided into three categories, according to: (1) the methods of application of AI used, (2) the industrial application of AI and (3) the system applications of AI.

As our aim is to establish the application of AI in the field of renewable energy, in this work we do not seek to derive an authorial definition of AI and adopt the one previously proposed by [20] and cited above. However, since AI is a combination of different methods and

application techniques, we will present some of the AI methods [23] in Table 1, as they also largely determine the direction of application of AI in the field of RE.

TABLE 1 ARTIFICIAL INTELLIGENCE METHODS

AI methods	Description
Machine learning (ML)	A basic AI method for machine learning, whereby by applying algorithms and models, interconnections in an existing data set are revealed and predictions are made.
Deep learning	A subset of ML specializing in hierarchical and in-depth analysis of large volumes of unstructured data through artificial neural networks.
Natural language processing	A method of understanding, interpreting, and generating human language by machines to facilitate interaction with humans.
Expert systems	AI programs mimicking the decision-making ability of experts from different fields.
Evolutionary algorithms	Algorithms exploring and refining potential solutions to complex optimization problems.
Reinforcement learning	AI reinforcement systems are an ML method in which agents are trained to make a series of decisions when interacting with a specific environment, for which they will receive a reward or penalties depending on the result obtained.
Probabilistic graphical models	A method in which, through a combination of probability theory and graphical models, a framework is created for reasoning under conditions of uncertainty and analysis of complex and complex dependencies.
Transfer learning:	A method in which a created model trained to solve a specific problem is applied as a starting point for solving another related problem.
Adversarial learning	A method for training AI to protect AI models and to assess the resilience of models.
Swarm intelligence	Method of using decentralized and self-organizing systems for collaborative problem-solving.

The cited AI training methods (see Table 1) include various techniques and strategies for solving complex and complex tasks. The application of any of the above is related to the nature of the problem encountered and the solution sought, which is why our analysis continues to identify the use of AI methods in the field of renewable energy. For the above, we will conduct bibliometric analysis and keyword co-occurrence analysis.

B. Methodology of the research

The data on which we build our research is obtained through Scopus. The large volume of critically reviewed scientific literature that the database contains provides a good basis for conducting a bibliometric analysis of the publications [24] at the intersection between renewable energy and artificial intelligence.

By applying keyword co-occurrence analysis, we establish the co-occurrence of keywords in the studied population and create networks of knowledge elements [25]. By analysing the citations of individual publications and their authors [26], we highlight the leading authors, their publications, the scientific journals in which there is the largest concentration of publications in the field under study, as well as the leading countries, authors of which have the largest number of scientific works.

To produce network maps through which we establish existing links between keywords and development trends, we use VOSviewer [27].

III. RESULTS AND DISCUSSION

To establish the relationship between artificial intelligence and renewable energy, we analyze scientific publications in Scopus for the period 2000-2025. Our search in “title-abstract-keywords” includes the terms “renewable energy” AND “Big Data” OR “machine learning” OR “artificial intelligence” OR “Deep Learning” OR “Neural Network*” OR “Granular Computing*” OR “Evolutionary Algorithm*” OR “Semantic Rule*” OR “Genetic Algorithm*”, following the example of [26]. As a result, we received 24,963 documents, of which we

excluded those that are not in English (n=767). We also limited the search according to the type of document, analysing only the results corresponding to document type “Article”.

A. Bibliometric performance analysis

Bibliometric performance analysis allows us to identify the leading authors whose research focuses on the possibilities of using artificial intelligence in renewable energy innovation. To do this, we use the metrics total number of posts and citations [24] - [28], which indicate respectively the amount of scientific production in each scientific field for the period of analysis (see Fig. 1) and the impact of this production on the scientific community.

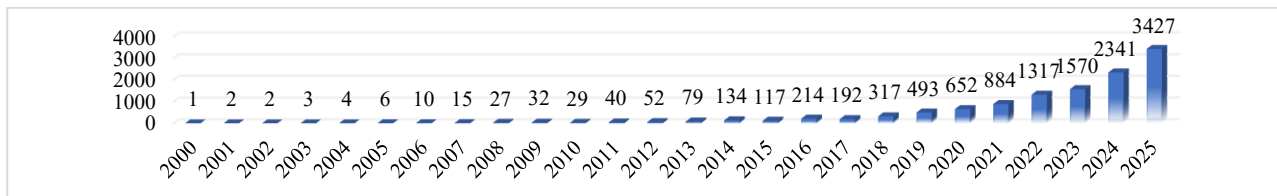


Fig. 1. Published research in Scopus in the field of RE [Own preparation based on Scopus data].

From the data constructed in this way (see Fig. 1), we establish a clearly outlined trend of growth in research activity, most pronounced in the period 2017-2025, when the number of published articles (n=7,338) increased annually by an average of 44.02%. Publications in 2025 accounted for 28.65% of all publications for the period 2000-2025, which proves the importance of the topics we have studied in modern times.

To illustrate the author's contribution to renewable energy and AI research, in Table 2 we present information about those authors who published the largest number of articles for the period 2000-2025.

TABLE 2 MOST PRODUCTIVE AUTHORS ON RE AND AI (2000-2025)

Rank	Authors	Documents	Total Citations	TC/D
1	Senjyu, T.	39	1080	27.69
2	Chen, Z..	35	2084	59.54
3	Guerrero, J. M.	29	1827	63
4	Bajaj, M.	25	754	30.16
	Yin, L.	25	314	12.56
5	Wang, R.	24	998	41.58
	Li, Y.	24	1396	58.17
6	Hu, W.	22	1391	63.23
	Deo, R. C.	22	1208	54.91
7	Khan, B.	21	497	23.67
	Sirano, P.	21	913	43.48
8	Hasanien, H .M.	20	1023	51.15
	Wang, Y.	20	958	47.9
9	Wang, J.	19	1472	77.47
	Hafeez, G.	19	1154	60.74
10	Huang, Q.	17	1294	76.12
	Jurado, F.	17	514	30.24
	Ogliari, E.	17	844	49.65

The total number of articles of the authors listed in Table 2 (416 publications) represents only 3.48% of the publication activity falling within the scope of the study (2000-2025). The fact that the most active researchers in the field of the intersection between renewable energy and artificial intelligence (see Fig. 2) make up such a small part of the population analysed testifies to the broad interest of the authors in the application of AI in the field of renewable energy.

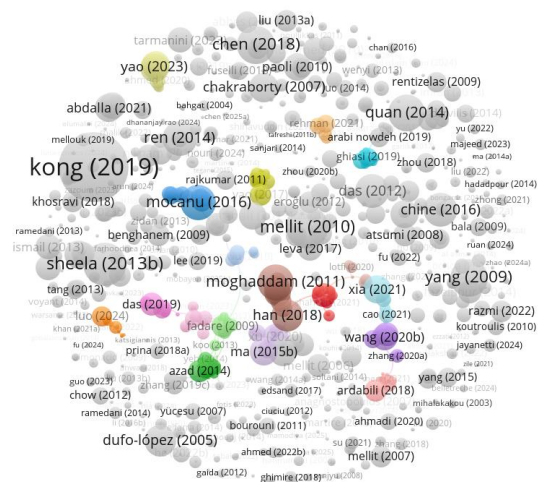


Fig. 2. Authors exploring the relationship between AI and RE [own preparation].

We are also interested in the publications that reported the highest citation rate during the analysis period, which is indicative of their importance among the academic community (see Table 3).

TABLE 3 THE 10 MOST CITED ARTICLES IN SCOPUS (2000-2025)

Rank	Articles	Total Citations
1	Short-term residential load forecasting based on lstm recurrent neural network [29].	2210
2	Review on methods to fix number of hidden neurons in neural networks [30].	838
3	A 24-h forecast of solar irradiance using artificial neural network: Application for performance prediction of a grid-connected pv plant at Trieste [31].	819
4	Model-free renewable scenario generation using generative adversarial networks [32].	659
5	Optimal design and techno-economic analysis of a hybrid solar-wind power generation system [33].	629
6	Short-term load and wind power forecasting using neural network-based prediction intervals [34].	627
7	Multi-objective operation management of a renewable mg (micro-grid) with back-up micro-turbine/fuel cell/battery hybrid power source [35].	593
8	Deep Learning for estimating building energy consumption [36].	574
9	Optimal parameters selection for bp neural network based on particle swarm optimization: A case of wind speed forecasting [37].	549
10	A novel fault diagnosis technique for photovoltaic system based on artificial neural networks [38].	526

From the information on the highest-citation publications (see Table 3), we find that the research topics are related to the possibilities of using AI for the design of systems for the production of renewable energy, prediction of RES performance, load forecasting, management of the operation of renewable micro-networks, fault diagnostic techniques, or AI can be applied in the entire spectrum of activities, related to RE.

To find out which are the scientific journals in which the authors publish their scientific achievements, we analyze those in which at least ten publications in the field of the subject we study have been published (see Table 4).

TABLE 4 THE 10 MOST PROLIFIC JOURNALS IN SCOPUS (2000-2025)

Rank	Journals	Documents	Total Citations
1	Energies	753	16187
2	IEEE Access	447	13556
3	Applied energy	430	22866
4	Energy	418	17599
5	Renewable energy technologies	327	16756
6	Sustainability (Switzerland)	252	4397
7	Energy conservation and management	198	13461
8	Journal of energy storage	197	4783
9	International Journal of electrical power and energy systems	188	7734
10	Energy reports	187	5272

The first four journals, which concentrate a significant part of the publications in the field we studied, published more than four hundred articles each for the period 2000-2025, reflecting the growing importance of research on the application of AI in the field of renewable energy. As expected, most authors have published their research in the journal *Energies*, bearing in mind that among the issues it addresses are those of technological development and engineering policy in the field of energy. In second position is *IEEE Access*, a multidisciplinary journal focused on applied engineering, innovative and experimental techniques, or research in emerging fields, which also includes research on AI and RE research. Third place is taken by *Applied energy*, whose areas of research are related to innovative solutions in the field of energy resources, their efficient and optimal utilization. The fourth position is occupied by *Energy*, whose focus is on research in the field of thermal energy and integrated energy systems, renewable energy, bioenergy, and their efficient use. The ranking is complemented by other significant journals, but due to their considerable number and our inability to present each of them in this analysis, we focus only on those with the highest recognition among researchers (see Table 4).

We complement the analysis with the publications that generated the highest citation among researchers, from which we can judge the importance of the journal for the formation and dissemination of significant innovative ideas (see Table 5).

TABLE 5 THE 10 MOST CITED JOURNALS IN SCOPUS (2000-2025)

Rank /Journals	Total Citations	Documents	TC/D
1. Applied energy	22866	430	53.18
2. Energy	17599	418	42.10
3. Renewable energy technologies	16756	327	51.24
4. Energies	16187	753	21.50
5. IEEE Access	13556	447	30.33
6. Energy conservation and management	13461	198	67.98
7. IEEE transactions on smart grid	7859	77	102.06
8. International Journal of electrical power and energy systems	7734	188	41.14
9. Journal of cleaner production	6916	126	54.89
10. Energy reports	5272	187	28.19

From the data in Table 5, we can see the citation of each of the sources and the number of documents that generated these citations. Comparing the data in Table 4 and Table 5, we see the emergence of two new sources: *IEEE transactions on smart grid* and *Journal of cleaner production*. Although these journals do not have a large concentration of publications, in *IEEE transactions on smart grid* we find the highest average citation rate (TC/D = 102.06), which expresses the weight and impact of the published research. The other journals that report a higher citation rate relative to the number of published articles are

Energy conservation and management (67.98), *Journal of cleaner production* (54.89) and *Applied energy* (53.18).

Information about other sources of scientific literature and their citation can be established from Fig. 3

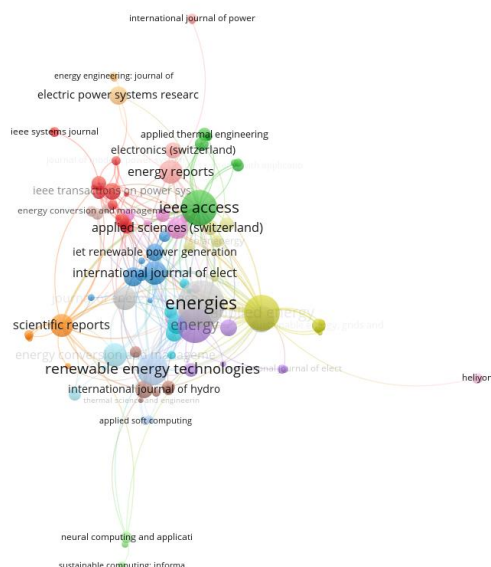


Fig. 3. Network map of most cited journals [own preparation].

To establish the contribution of the individual countries from which the analysed activity derives, we present the countries (see Fig. 4) whose authors have published the largest number of studies. The nationality of the researchers is indicative of the commitment not only of individuals, but also of society, politicians, and institutions in finding answers to questions that are significant for modern development, in this case – the relationship between AI and RE.

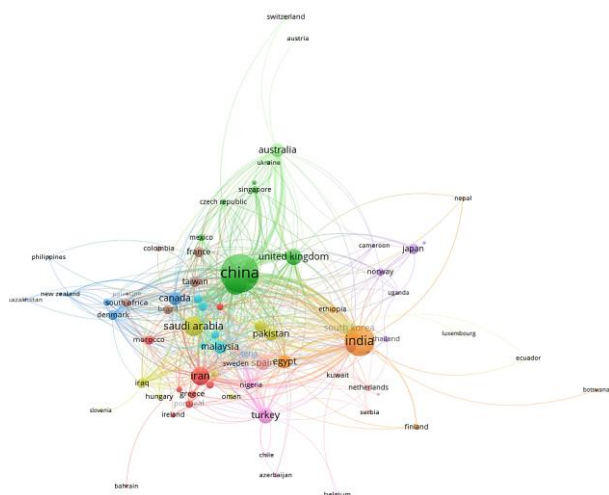


Fig. 4. Network map of sources of publication activity [own preparation].

From the network map of the countries that source publication activity (see Fig. 4), we can judge that China has made the greatest contribution to the development of research at the intersection between artificial intelligence

and renewable energy (3,222 documents, 83,736 citations). In second place is India (1,972; 34,984), and in third place is the United States (1,033; 36,382). The reported three times stronger activity of authors from China, compared to those from the United States, expresses not only the efforts, but also the capacity and commitment of Chinese researchers to develop both computer technologies and those in the field of renewable energy sources. At the same time, the average citation TC/D of publications by authors from the United States is higher compared to that of authors from China ($TC/D_{USA}=35.22$; $TC/D_{CHINA}=25.99$). The ranking is complemented by countries such as: Saudi Arabia (847 articles; 20,675 citations); Iran (722; 25,078); United Kingdom (582; 20,987), Turkey (536, 12,884), etc.

B. Keywords co-occurrence analysis

When analysing the keywords indicated in the articles on which our analysis is built, we establish the thematic area in which the publications fall. We apply a “co-occurrence” analysis in all “author keywords” in a full count and use VOSviewer to create a network map of the relationships between the keywords (see Fig. 5). The total number of keywords that VOSviewer generates is 47,903, which is indicative of the wide range of topics of interest to researchers regarding the application of AI in the field of renewable energy. To clear the visual map, we only include keywords that appear more than ten times in the analysed array. This criterion is met by 2,587 keywords, of which VOSviewer calculates and visualizes 1,000, the strength of the relationships between which is the greatest. Table 6 lists the top ten keywords of the set thus defined.

TABLE 6 KEYWORD OCCURRENCES

Nº	Keywords	Occurrences	Total link strength
1	Renewable energy technologies	3,448	40,500
2	Renewable energy resources	2,404	31,601
3	Renewable energies	2,524	31,211
4	optimisations	2,134	28,291
5	Machine learning (ml)	2,515	28,230
6	Genetic algorithms	2,035	24,941
7	Forecasting	1,745	23,206
8	Alternative energy	1,560	21,816
9	Renewable energy sources	1,721	21,795
10	Neural-networks	1,763	20,663

With VOSviewer, we illustrate the grouping of keywords in a network map (see Fig. 5), which allows us to find the relationships between the keywords used by the authors. VOSviewer calculates the frequency with which individual keywords appear together using the association

strength method. Thus, by applying algorithms, a specific distribution and grouping of keywords is sought in order to maximize the density of links in individual clusters. The size of the node indicates the frequency of occurrence of the keyword among the analysed articles.

As can be seen from Fig. 5, the keywords are divided into five clusters. The largest of them, **red cluster**, includes 247 keywords, with the most frequently appearing keywords being “renewable energies” (2524), “machine learning” (2515), “neural-networks” (1763), “forecasting” (1754), “deep learning” (1672), “wind power” (1498), “artificial neural network” (1322), “learning system” (1270), “solar energy” (1215), which expresses the application of various methods and techniques in the composition of AI to predict the productivity, efficiency gains and renewables load management.

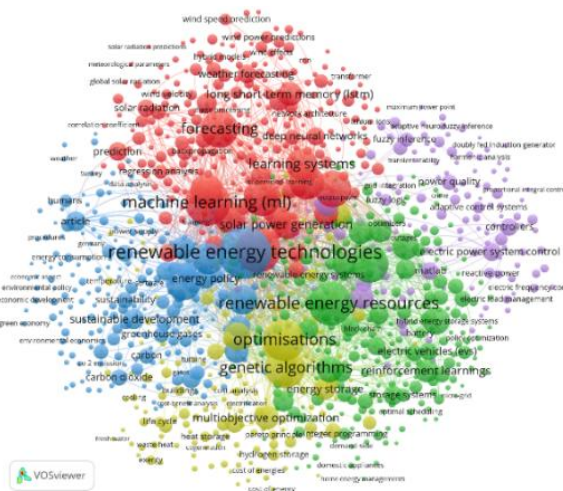


Fig. 5. Keyword Network Map [own preparation].

The second **green cluster** includes “renewable energy resources” (2404), “renewable energy sources” (1721), “microgrids” (975), “electric power transmission networks” (887), “energy management” (847), “smart power grids” (677), “reinforcement learnings” (674), as well as topics related to the application of various AI techniques to create smart grids. The third **blue cluster** covers 217 keywords, the most used of which are “renewable energy technologies” (3448), “alternative energy” (1560), “energy” (1109), “artificial intelligence” (1249), “energy utilization” (715), “decision making” (659), “algorithm” (627), “sustainable development” (553), “fossil fuels” (476) etc. The focus here is on renewable energy, in the context of the concept of sustainable development, environmental impact and waste and carbon management, as well as the application of AI to increase the efficiency of these processes and achieve the Sustainable Development Goals. The fourth **yellow cluster** covers the terms “optimisations” (2134), “genetic algorithms” (2035), “energy efficiency” (944), “multiobjective optimization” (711) “wind turbines” (619), “energy storage” (605), “energy systems” (434), “sensitivity analysis” (323), which reveal the application of genetic algorithms for the development of alternative solutions, planning and optimization of energy storage capacity, increasing the energy efficiency of RES, cost

optimization. In the fifth **purple cluster**, the emphasis is placed on “photovoltaic (pv)” (719), “particle swarm optimization (psa)” (698), “electric power system control” (409), “controllers” (394), “matlab” (376), “optimization algorithms” (335), “power quality” (302), “fuzzy system” (253), which highlights the use of artificial intelligence environments to design and simulate engineering solutions, applying fuzzy logic in AI to decision-making related to controlling, managing and optimising the operation of photovoltaic systems and other sources of RE.

To establish the trends in the development of AI applications in the field of RES, we present an overlay visualization of the keywords (see Fig. 6) used in the period 2019-2025, when we found the strongest publication activity.

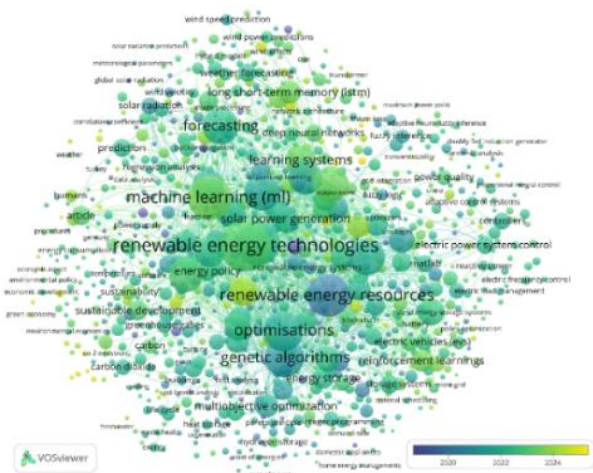


Fig. 6. Keywords overlay visualization [own preparation].

Visible from the network card, the earliest terms such as “photovoltaic cells”, “electric power generation”, “electric power system”, “optimization problems”, “algorithms”, “modelling”, “computer simulation”, “decision support system”. In 2020, researchers’ interest is focused on „renewable energy resources”, “wind”, “solar radiation”, “distributed power generation”, electric utilities”, and “genetic algorithms”, “evolutionary algorithms”, “scheduling”. For 2021, the emphasis is placed on research on the optimization of existing systems, “multiobjective optimization”, “costs”, “wind power”, “electric power transmission networks”, “solar energy”, “renewable energy sources”, and “neural-networks”, “artificial neural networks”, “fuzzy systems”, “forecasting methods”, “controllers”. In the active phase of research, in 2022, we are seeing an increase in the use of AI to predict the weather and determine the capacity of renewable sources “prediction”, “forecasting”, “weather forecasting”, “climate change”, “photovoltaics”, “wind speed”, “artificial intelligence”, “learning algorithms”, “alternative energy”, “energy efficiency”, “energy utilization”, “energy storage”, “energy management system”, “microgrid”, “sustainable development”, “digital storage”. In 2023, the focus is on renewable energy technologies affecting “carbon emission”, “energy systems”, “hybrid renewable energy” and the possibilities for applying AI through “learning system”, “machine

learning”, “deep learning”, “convolutional neural network”, “long-short term memory”, “reinforcement learnings”, “deep reinforcement learnings”, “predictive models”. For 2024, the authors' interest is focused on energy and its sources “energy”, “clean energy”, “thermal”, “solar fuels”, “windmill”, “wind power integration”, “hybrid power”, and, on the other hand, AI is presented through “short term memory”, “wind forecasting”, “adversarial machine learning”. It also raises the question of „green development“, „sustainable development goals“, and the extent to which renewable energy meets sustainable development „zero carbon“, „carbon capture and utilization“, „low emission“, and can contribute to the achievement of the Sustainable Development Goals.

The analysis of these topics continues into the next year, although we expect the emergence of new areas of study, due to the lack of visualization of keywords appearing more than ten times in the analysed population with a year of publication 2025.

IV. CONCLUSIONS

Through the proposed research, we have not only outlined the role of AI in the development of the renewable energy sector but also revealed some of the methods by which AI can be applied in the field of unconventional energy. As a result of the goals and objectives of the research, we conducted bibliometric analysis and keyword co-occurrence analysis, identifying the areas of application of AI in the field of renewable energy. We also highlighted the researchers and their most significant publications that found the widest response among the scientific community in the period 2000-2025.

Analysing the network map of keywords (see Fig. 5), we found that each cluster includes both different renewable energy sources and different AI methods that can be applied to increase the efficiency and operation capacity of renewable energy. This allows us to say that the scientific community is directly involved in identifying areas for application of AI in the field of RE and in revealing the advantages of implementing AI methods to increase energy efficiency.

By tracking the development trends of RE and AI research, we found that the last years of the analysed period (2019-2025) marked considerable progress in terms of areas of application of AI. Judging by the keywords overlay visualization (see Fig. 6), we formulate conclusions about the development of the application of AI in the field of RES for each individual year of the active research work of the analysed set of researchers, as follows:

- In 2019, AI is being applied in the form of algorithms and computer simulations to support the energy system.
- In 2020, through the application of genetic algorithms, opportunities are sought for optimization of the activity of renewable energy sources, creation of schedules for maximum use of solar and wind energy.

- For 2021, the issue of optimization of existing systems is deepening and multiobjective optimization is being conducted through artificial neural networks in relation to renewable energy sources. The possibility of predicting the time and controlling the operation of RES is also being investigated.
- A characteristic of 2022 is that methods for predicting weather and climate change are at the heart of the analysed research. Questions are also raised about the efficiency of management and use of RE, and the possibility of its storage. Microgrids are also considered as standalone energy grids.
- In 2023, interest in renewable energy technologies and the application of AI training systems is deepening (“machine learning”, “deep learning”, “convolutional neural network” “reinforcement learnings”, “deep reinforcement learnings”, “long-short term memory”) to solve complex problems in the field of RE.
- In 2024, the authors' view goes beyond the limits of renewable energy, considering the priority consideration of the issue of clean energy, hybrid energy, zero carbon, and the Sustainable Development Goals. This is where the “adversarial machine learning” is used, which signals the commitment of researchers to create trustworthy AI systems by exploring ways to deceive and manipulate it to limit attacks and external intentional and negative impacts on RES.
- In 2025, new areas of research are emerging at the intersection between AI and BE, the development of which we will analyze in the future.

The prepared analysis and the results of the proposed study firmly emphasize the capabilities of AI to reduce the identified negative effects of RES. They can also be used as a basis for future research to identify the development of AI applications in the field of ER. At the same time, they also represent a useful indicator of the commitment of the scientific community to expand the boundaries of two of the most significant areas of development of society in recent decades.

Beyond the focus of the current study and subject to future analysis is a more detailed analysis of the publication activity conducted during the period of analysis.

ACKNOWLEDGMENT

This article was published with the financial support of Technical University of Gabrovo, Bulgaria under project NIP2026-11 “Benchmarking for Integrating Artificial Intelligence into Strategic Company Management”.

REFERENCES

- [1] R. Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Viking Press, 1990.
- [2] M. L. Minsky, *Semantic information processing*. Cambridge, MA: MIT Press, 1986.

- [3] A. Harjanne, J. Korhonen, "Abandoning the concept of renewable energy," in *Energy Policy*, 127, 2019, pp. 330-340.
- [4] A. G. Olabi, M. A. Abdelkareem, "Renewable energy and climate change," in *Renewable and Sustainable Energy Reviews* 158, 2022, pp. 1-7.
- [5] M. Makešová, M. Valentová, "The Concept of Multiple Impacts of Renewable Energy Sources: A Critical Review," *Energies* 14, 2021, 3183, [Accessed April 15, 2026], <https://doi.org/10.3390/en14113183>.
- [6] N. Ivanova, P. Datta, "The environmental impact of renewable energy," in *International Journal of Business and Economic Development*, Vol.11, 2023, pp. 85-103.
- [7] A. Rashidov, "Determining of the degree of intelligence of artificial intelligence systems," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1-6, [Accessed April 1, 2026], DOI: [10.1109/ICCCNT56998.2023.10307831](https://doi.org/10.1109/ICCCNT56998.2023.10307831).
- [8] A. F. Borges, F. J. Laurindo, M. M. Spínola, R. F. Gonçalves, C. A. Mattos, "The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions," in *International journal of information management*, 57, 2021. 102225. ISSN 0268-4012.
- [9] O. Mypati, A. Mukherjee, D. Mishra, S. K. Pal, P. P. Chakrabarti, A. Pal, "A critical review on applications of artificial intelligence in manufacturing," in *Artificial Intelligence Review*, 56(Suppl 1), 2023, pp. 661-768, [Accessed April 18, 2025], <https://doi.org/10.1007/s10462-023-10535-y>.
- [10] T. Rachovski, D. Petrova, I. Ivanov, "Automated creation of educational questions: Analysis of artificial intelligence technologies and their role in education," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*. Vol. 2. 2024, pp. 465-467, [Accessed April 1, 2025], <https://doi.org/10.17770/etr2024vol2.8101>.
- [11] M. R. Anwar, L. D. Sakti, "Integrating Artificial Intelligence and Environmental Science for Sustainable Urban Planning," in *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 5(2), 2023, pp. 179-191, Available: <https://aptikom-journal.id/itsdi/article/view/666>, [Accessed April 15, 2025].
- [12] R. Hirani, K. Noruzi, H. Khuram, A. S. Hussaini, E. I. Aifuwa, K. E. Ely, J. M. Lewis, A. E. Gabr, A. Smiley, R. K. Tiwari, et al. "Artificial Intelligence and Healthcare: A Journey through History," in *Present Innovations, and Future Possibilities*. Life 2024, 14, 557, [Accessed April 15, 2025], <https://doi.org/10.3390/life14050557>.
- [13] I. Ivanov, K. Petrov, T. Rachovski, D. Petrova, "Methodological and Applied Aspects of Artificial Intelligence in Energy Consumption Prediction," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 2, 2025, June, pp. 165-169, [Accessed January 15, 2026], <https://doi.org/10.17770/etr2025vol2.8601>.
- [14] A. Rashidov, F. Rashidova, "Challenges and limitations in the use of artificial intelligence in research and some options to overcome them," in 2024 15th International Conference on Computing Communication and Networking Technologies, ICCNT, IEEE, 2024. p. 1-4., [Accessed April 15, 2025], DOI: [10.1109/ICCCNT61001.2024.10724588](https://doi.org/10.1109/ICCCNT61001.2024.10724588).
- [15] I. Balabanova, D. Petrova, G. Georgiev. "Recognition of Face Images by DWT, NB, SVM, FFNN and CFNN Methodology," in 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). IEEE, 2024, [Accessed June 15, 2025], DOI: [10.1109/CIEES62939.2024.10811433](https://doi.org/10.1109/CIEES62939.2024.10811433).
- [16] N. Nikolova, "Key business priorities and good practices of industrial management," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, vol. 1, June 2025, pp. 411-415, [Accessed April 14, 2026], <https://doi.org/10.17770/etr2025vol1.8620>.
- [17] D. Petrova, N. Nikolova, "Innovative development and competitiveness of the industrial sector in Bulgaria," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 4, 2025, June, pp. 297-30, [Accessed March 14, 2026], <https://doi.org/10.17770/etr2025vol4.8397>.
- [18] N. Nikolova, "Industry 4.0-development and consequences for sustainable development of Bulgaria," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 3, 2021, June, pp. 245-251, [Accessed March 27, 2024], <https://doi.org/10.17770/etr2021vol3.6543>.
- [19] V. Boeva, "The Integration of the Digital Economy and the Green Transition—Opportunities for Small and Medium-Sized Enterprises," in *Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference*, Vol. 1, 2025, June, pp. 97-102, [Accessed March 30, 2026], <https://doi.org/10.17770/etr2025vol1.8657>.
- [20] M. Haenlein, A. Kaplan, "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence," in *California Management Review*, 61(4), 2019, pp. 5-14, [Accessed January 10, 2026], <https://doi.org/10.1177/0008125619864925>.
- [21] V. Nikolova-Minkova, "Historical development of technologies in the field of Artificial Intelligence," in *Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference*. Volume II, 2025, pp. 243-250, [Accessed April 15, 2026], <https://doi.org/10.17770/etr2025vol2.8609>.
- [22] S. Bahoo, M. Cucculelli, D. Qamar, "Artificial intelligence and corporate innovation: A review and research agenda," *Technological Forecasting and Social Change*, Volume 188, 122264, ISSN 0040-1625, 2023, [Accessed February 05, 2025], <https://doi.org/10.1016/j.techfore.2022.122264>.
- [23] M. Elahi, S. O. Afolaranmi, J. L. Martinez Lastra, J. A. Perez Garcia, "A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment," in *Discover artificial intelligence*, 3(1), 2023, 43, [Accessed December 15, 2024], <https://doi.org/10.1007/s44163-023-00089-x>.
- [24] I. Passas, "Bibliometric Analysis: The Main Steps," in *Encyclopedia*, 4, 2024, pp. 1014-1025. [Accessed April 15, 2025], <https://doi.org/10.3390/encyclopedia4020065>.
- [25] A. Rejeb, K. Rejeb, I. Zrelli, E. Süle, "Industry 5.0 as seen through its academic literature: an investigation using co-word analysis," in *Discover Sustainability*, 6(1), 2025, 307, [Accessed April 3, 2026], <https://doi.org/10.1007/s43621-025-01166-0>.
- [26] S. Raut, N. U. I. Hossain, M. Kouhizadeh, S. A. Fazio, "Application of artificial intelligence in circular economy: A critical analysis of the current research," in *Sustainable Futures*, 9, 2025, 100784, [Accessed April 15, 2026], <https://doi.org/10.1016/j.sfsr.2025.100784>.
- [27] N. J. Van Eck, L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," in *Scientometrics*, 84(2), 2010, pp. 523-538, [Accessed April 1, 2024], <https://doi.org/10.1007/s1192-009-0146-3>.
- [28] A. F. J. Van Raan, "Advances in bibliometric analysis: Research performance assessment and science mapping," in *Bibliometrics: Use and Abuse in the Review of Research Performance*; Blockmans, W., Engwall, L., Weaire, D., Eds.; Portland Press Ltd.: London, UK, Volume 87, 2014.
- [29] W. Kong, Z. Y. Dong, Y. Jia, D. J. David, Y. Xu, Y. Zhang, "Short-term residential load forecasting based on lstm recurrent neural network," in *IEEE Transactions on smart grid*, 10(1), 2019, pp 841-851, [Accessed April 1, 2024], DOI: [10.1109/TSG.2017.2753802](https://doi.org/10.1109/TSG.2017.2753802).
- [30] K. G. Sheela, S. N. Deepa, "Review on methods to fix number of hidden neurons in neural networks," in *Mathematical problems in engineering*, 2013 (1), 11 pages, 425740.
- [31] A. Mellit, A. M. Pavan, "A 24-h forecast of solar irradiance using artificial neural network: Application for performance prediction of a grid-connected pv plant at Trieste, Italy," in *Solar Energy*, 84(5), 2010, pp. 807-821.
- [32] Y. Chen, Y. Wang, D. Kirschen, B. Zhang, "Model-free renewable scenario generation using generative adversarial networks," in *IEEE transactions on power system*, 33(3), 2018, pp.3265-3275.

- [33] H. Yang, Z. Wei, L. Chengzhi, Optimal design and techno-economic analysis of a hybrid solar-wind power generation system, in *Applied Energy*, 86(2), 2009, pp. 163-169.
- [34] H. Quan, D. Srinivasan, A. Khosravi, "Short-term load and wind power forecasting using neural network-based prediction intervals," in *IEEE transactions on neural networks and learning systems*, 25(2), 2014, pp.303-315.
- [35] A. A. Moghaddam, A.Seifi, T. Niknam, M. R. A. Pahlavani, "Multi-objective operation management of a renewable mg (micro-grid) with back-up micro-turbine/fuel cell/battery hybrid power source," in *Energy*, 36(11), 2011, pp.6490-6507.
- [36] E. Mocanu, P. H. Nguyen, M. Gibescu, W. I. Kling, "Deep Learning for estimating building energy consumption," in *Sustainable energy, grids and networks*, 6, 2016, pp. 91-99.
- [37] C. Ren, N. An, J. Wang, H. Lian, B. HU, D. Shang, "Optimal parameters selection for bp neural network based on particle swarm optimization: A case of wind speed forecasting," in *Knowledge-based system*, 56, 2014, pp. 226-239.
- [38] W. Chine, A. Mellit, V. Lughi, A. Malek G. Sulligoi, A. Massi, "A novel fault diagnosis technique for photovoltaic system based on artificial neural networks," in *Renewable energy*, 90, 2016, pp.501-512.

Comparative Analysis of Deep Learning Architectures for Monochromatic Image Colorization

Ihor Panasenko

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
ihor.panasenko1@nure.ua

Kirill Smelyakov

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
kyrylo.smelyakov@nure.ua

Anastasiya Chupryna

Software engineering department
Kharkiv National University of
Radioelectronics
Kharkiv, Ukraine
anastasiya.chupryna@nure.ua

Paulius Sakalys

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
p.sakalys@eif.viko.lt

Loreta Savulioniene

Faculty of Civil Engineering
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
l.savulioniene@viko.lt

Dainius Savulionis

Faculty of Electronics and
Informatics
Vilniaus kolegija
Higher Education Institution
Vilnius, Lithuania
d.savulionis@eif.viko.lt

Abstract – colorizing monochromatic images is crucial for enhancing the informativeness of visual data in modern information technology and computer vision systems. However, automatic colorization poses an inherently ill-posed mathematical challenge due to the multimodal nature of color distributions, where multiple valid color mappings exist for any given grayscale input. This article conducts a comparative analysis of classical algorithms (such as the Welch and Levin methods) against advanced deep learning pipelines. The evaluated architectures range from baseline convolutional neural networks (CNNs) and standalone U-Net models to generative adversarial networks (GANs) and a novel hybrid Fusion GAN that integrates global semantic priors extracted via a ResNet-18 backbone. All models were trained and rigorously evaluated in the CIE Lab* color space, which effectively separates luminance from chrominance. To ensure a robust evaluation, experiments were conducted using a diverse benchmark of 2,000 images from the COCO dataset. Quality assessment combined traditional metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) with the Learned Perceptual Image Patch Similarity (LPIPS) metric, prioritizing human-like visual fidelity. Experimental results yielded counterintuitive insights. While the proposed Fusion GAN successfully surpassed classical methods, baseline CNNs, and standard GANs across most benchmarks, the standalone U-Net architecture secured the highest overall ranking. Specifically, U-Net achieved the top SSIM score of 0.945 (indicating superior structural preservation), the lowest LPIPS of 0.180 (best perceptual quality), and the fastest inference speed, enabling real-time applications.

Keywords – computer vision, image colorization, deep learning, GANs, U-Net, CNNs, LPIPS, SSIM, PSNR, COCO dataset.

I. INTRODUCTION

Restoring color to black-and-white images is much more than just a visual update or cosmetic restoration. In fields such as medicine, historical archive processing, restoration of old photographs, or analysis of satellite data, color plays a key role in understanding what exactly is depicted in the image [1]. The quality and accuracy of such processing directly affect the effectiveness of any subsequent analysis in computer vision systems [2]. However, from a mathematical standpoint, colorization remains a complex task: since the L* luminance channel does not contain information about hues, the same photo can be colored in an infinite number of ways.

Previously, attempts were made to solve this problem using user input. For example, the Welch algorithm transferred colors from a similar reference image based on texture [3], while the Levin method “blended” color between neighboring pixels with similar brightness [4]. Both of these approaches yielded consistent results, provided that the user’s instructions were accurate, but at the same time required a lot of manual work, which made automatic processing of large archives impossible.

The transition to data-driven methods began with CNN-based approaches [5], followed by encoder-decoder

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.217>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

architectures with skip connections [6], conditional GANs [7][8], and most recently transformer-based models [9]. Each generation reduced a specific failure mode but introduced new trade-offs between accuracy, perceptual realism, and inference speed.

Despite these successes, in practice, it is still difficult to find the ideal balance between image realism, accuracy, and system performance. This work proposes our own solutions to these challenges by developing Fusion GAN. We proposed a model that uses semantic cues from the ResNet-18 network [10] to better understand the overall context of the image.

II. RELATED WORK

Classic algorithms. Semi-automatic colorization methods dominated early research. The Welch algorithm transferred hues from a reference color image by matching texture and luminance in the Lab color space [3], while the Levin method propagated user-applied color strokes to neighboring areas with similar brightness [4]. Both approaches were computationally light but required significant manual input, making fully automated archive processing infeasible.

The era of convolutional neural networks (CNNs). Zhang et al. reframed colorization as per-pixel classification over 313 quantized ab bins, avoiding the dominance of desaturated "safe" tones and substantially increasing output vibrancy [5]. Iizuka et al. extended this with a dual-stream architecture – one branch capturing global scene context, the other capturing local texture – a design principle that directly motivates the Fusion GAN model [11] explored in this work.

Encoder-decoder architectures and skip connections. U-Net [6] introduced long skip connections between encoding and decoding layers, allowing fine spatial detail to bypass heavy compression stages and significantly reducing color bleeding at object boundaries. Stable training of such deep architectures depends critically on proper weight initialization; biologically inspired stochastic initialization strategies accelerate convergence and prevent neuron saturation [12].

Conditional Generative Adversarial Networks (cGANs). The Pix2Pix framework [7][8] radically transformed colorization from a regression task into an adversarial image-translation process; its PatchGAN discriminator recovers vivid textures and color transitions typically lost by L1 regression. DeOldify further refined this approach with Self-Attention mechanisms and a NoGAN pre-training strategy, achieving strong results on historical photographs.

Transformers and diffusion models. DDColor [9] combines a pixel decoder with a query-based transformer color decoder, leveraging cross-attention to reduce inter-object color bleeding artifacts. Diffusion models treat colorization as iterative denoising and often surpass GANs in quality, but require 50–1,000 inference steps – prohibitive for interactive web applications where real-time visual processing is essential.

Evaluation metrics. PSNR and SSIM measure pixel-level and structural fidelity but correlate poorly with human perception. The LPIPS metric [13], calibrated against large-scale human similarity judgments via deep feature distances, is now the standard perceptual quality measure. This work applies all three metrics in combination to capture the trade-offs that no single score can reveal.

III. METHODOLOGY

A. Color Space and Problem Statement

All models under study operate in the CIE Lab* color space. This color space was chosen because it allows for a perfect separation of information regarding luminance and color. The L* luminance channel (normalized from 0 to 1) serves as the sole input to the neural network, and the model's task is to predict the two color channels: a* and b* (normalized from -1 to 1 using the Tanh function).

From a mathematical standpoint, we train the function (1), which must reconstruct realistic shades based solely on luminance data.

$$f: L \rightarrow (a, b) \quad (1)$$

The choice of the Lab color space is due to its “perceptual uniformity”: equal mathematical distances within it roughly correspond to how the human eye perceives differences between colors. It is also important that the L* channel remains unchanged during processing, which guarantees the complete preservation of the structure and sharpness of the original image [5].

B. Dataset and Preprocessing

For our experiments, we used the validation set of the COCO 2017 dataset. From this, we formed a training subset of 2,000 images (random selection), which we split in a 90/10 ratio for training and validation, respectively. The choice of COCO is explained by the enormous variety of objects – over 80 categories. This allows us to test how well the architectures capture the scene context without being tied to a narrow topic (e.g., only faces or only landscapes).

Data preprocessing included resizing to 256×256 pixels and conversion to the Lab format (D65 white point standard). To improve model robustness during training, augmentation was applied: random cropping and horizontal mirroring of frames.

C. Architectures

Basic CNN. This model is built on the principle of a symmetric encoder-decoder, but without using feed-through connections. The process works as follows: four blocks compress the input data to a minimal size (bottleneck), after which four transposed convolution blocks attempt to reconstruct the color map ab.

We trained this network using the standard loss function MSE (L2). In our work, this model serves as a baseline: it clearly demonstrates the main drawback of simple regression – the desaturation or “sepia” effect. Since the model attempts to minimize the mean error when faced with ambiguity, it selects the “safest” gray color [5].

U-Net. The next stage of our research was the classic U-Net architecture [6]. It has eight downsampling stages and seven upsampling stages, allowing the input data to be compressed into a $1 \times 1 \times 512$ bottleneck. The main feature of this model is its long skip connections: they transmit feature maps from each encoder layer directly to the corresponding decoder layers. This ensures that when assigning colors, the neural network clearly focuses on object boundaries regardless of the resolution level. The final layer of the system uses bilinear upsampling in combination with the Tanh function.

For training, we chose the L1 (MAE) loss function. The stability of such a deep network is ensured by a special strategy for stochastic weight initialization, inspired by biological neural systems [12]. This solution helps the model converge better during training and minimizes the risk of activations “getting stuck” in the deep layers of the encoder-decoder.

Conditional GAN (cGAN / Pix2Pix). In this model, we transition from simple regression to adversarial training [8]. The role of the Generator here is performed by the U-Net described above, while the Discriminator of the PatchGAN architecture [7] is responsible for evaluating the results. Its structure includes blocks of progressive resolution reduction and a final layer that outputs a score for individual image patches (fragments). The discriminator analyzes the pair $(L, ab_{predicted})$ and attempts to determine whether the color map is real or fake.

The total loss function of the Generator (2) is as follows:

$$L_G = L_{GAN}(G, D) + \lambda_{L1} \cdot L_{L1}(G) + \lambda_P \cdot L_{per}(G) \quad (2)$$

where $\lambda_{L1} = 100$ (according to [7]), and L_{per} is the perceptual loss based on feature matching from the VGG-16 network at layers $\{3, 8, 15, 22\}$ [14]. To train the Discriminator, we used BCEWithLogitsLoss with one-sided label smoothing (the “true” value = 0.9). Both networks were optimized using the Adam algorithm with the following parameters: $lr = 2 \times 10^{-4}$, $\beta_1 = 0.5$, $\beta_2 = 0.999$.

Fusion GAN. This architecture is an extension of cGAN, where we added a mechanism for understanding global context. To do this, we integrated the base ResNet-18 network [10], adapting its first layer to work with single-channel brightness (by averaging the weights of pre-trained RGB filters). The U-Net encoder generates a feature vector, which is fused at the “bottleneck” with a 512-dimensional global hint from ResNet-18. The final fused vector is formed through a linear layer with a ReLU function (3):

$$z_{fused} = ReLU(W_f \cdot [z_{enc}; g_{global}]) \quad (3)$$

After that, the fused vector is passed to the decoder for the final image reconstruction. The ResNet-18 base network is trained jointly with the generator, while the discriminator and loss functions remain the same as in the cGAN stage. This principle of multi-branch data fusion has

proven effective not only in colorization but also in many other critical computer vision tasks [11][15].

D. Evaluation Metrics

To objectively verify the results, we use three complementary metrics:

- PSNR (Peak Signal-to-Noise Ratio). This metric measures the technical accuracy of reconstruction at the pixel level. The higher the PSNR value (in decibels), the fewer digital distortions in the image.
- SSIM (Structural Similarity Index). This metric evaluates how well the model has preserved the brightness, contrast, and overall structure of objects. The value ranges from 0 to 1, where a higher score indicates a better match to the original.
- LPIPS (Learned Perceptual Image Patch Similarity) [13] is a modern measure of perceptual similarity, calibrated to reflect how a human evaluates an image. Unlike the previous metrics, a lower value is better here, as it indicates high naturalness and realism of colors.

We consider it critically important to analyze this data holistically. For example, a “conservative” model may achieve a high PSNR simply because it selects muted, almost gray colors (minimal pixel error), but its LPIPS score will be low due to a lack of realism. At the same time, generative adversarial networks (GANs) often produce vibrant colors, which improves LPIPS, but may suffer from the appearance of artifacts that lower SSIM.

IV. EXPERIMENTAL RESULT

A. Quantitative Comparison

The results that were received after running test colorizing on the set of images with different scenes that were not included in the learning dataset are illustrated in Table I.

TABLE I. QUANTITATIVE EVALUATION ON VALIDATION SUBSET

Architecture	PSNR (dB)	SSIM	LPIPS	Inference (ms)
Baseline CNN	~22.0	0.71	0.38	~22
U-Net	28.53	0.945	0.180	~118
cGAN	~24.5	0.887	0.165	~120
Fusion GAN	~24.1	0.881	0.168	~130

For the PSNR and SSIM metrics, a higher value indicates a better result, whereas for the LPIPS metric and inference time, a lower value is better. As can be seen from the data, the U-Net architecture delivers the best overall performance across all metrics simultaneously within a training budget of 20 epochs.

B. Baseline CNN

The typical errors of a basic convolutional network have a clear mathematical explanation: they are a direct consequence of using the L2 loss function. When faced with ambiguity in color selection, the network simply averages all possible options. As a result, instead of vivid hues, we get dull gray-brown patches – the so-called “sepia effect” [5]. Furthermore, since this model lacks skip connections, it loses information about fine details, causing colors to often bleed beyond object boundaries. This is confirmed by the numbers: a gap in the PSNR metric of over 6 dB compared to U-Net indicates both low accuracy at the level of individual pixels and serious overall structural distortions.

C. U-Net

The advantage of the U-Net architecture is based on two key mechanisms. First, skip connections transmit accurate information about object boundaries at all stages of processing, ensuring that the generated color perfectly matches the contours [6]. Second, the use of the L1 loss function helps partially mitigate the problem of washed-out colors characteristic of L2. As a result, we obtain structurally accurate images with high generation speed (approximately 118 ms per frame when using a CPU). This speed makes the model an excellent choice for interactive systems where response time is critical [2]. However, the tendency toward loss of saturation still remains, especially in large homogeneous areas (e.g., sky or water), where the network again tends toward averaged “safe” shades due to a lack of chromatic cues.

D. Conditional GAN

Unlike U-Net, the cGAN competitive approach forces the model to abandon “safe” averaging. By analyzing the image in separate fragments (patches), the network successfully restores bright and saturated textures where U-Net produces muted tones – for example, green grass, illuminated surfaces, or patterned fabrics [7]. But this approach has its drawbacks. Since the PatchGAN discriminator evaluates only small local areas, it often loses the overall context of the scene. A fragment on its own may look realistic, but noticeable color artifacts appear when viewed across the entire photo (for example, unnatural spots on skin or clothing).

It is precisely because of such errors that the SSIM structural similarity metric in cGAN is lower than in U-Net (0.887 vs. 0.945). However, the better result on the LPIPS metric (0.165 vs. 0.180 in U-Net) convincingly demonstrates: although GAN loses out in terms of mathematical pixel accuracy, from the perspective of human perception, it generates a significantly more vivid and natural image.

E. Fusion GAN

Using global hints from the ResNet-18 network in the Fusion GAN model [10] allowed the system to recognize the general content of an image much better. This is particularly noticeable in scenes with clear semantics – for example, in landscapes, images of food, or animals with distinctive coloring. In such cases, the results are globally

consistent and appear more natural than those from the standard cGAN architecture.

In terms of numerical metrics, COCO Fusion GAN demonstrates results close to those of cGAN. This can be explained by the limited training budget (20 epochs) and small sample size (1,800 images), which proved insufficient to fully leverage all the benefits of the additional fusion parameters. However, the very principle of multi-branch feature fusion has already proven its high effectiveness in other complex tasks, such as traffic accident detection systems, where accurate visual perception is critical for safety [15]. This confirms that the architectural approach we have chosen is promising and goes far beyond the scope of the colorization task alone.

F. Qualitative Observations

One image was selected and colorized for a qualitative (visual) analysis. The selected image contains complex multi-subject scene, featuring people against a backdrop of architectural structures and greenery. Fig. 1 shows the original color image, which serves as a reference for comparison.



Fig. 1. Original color image

The numerical results of the colorization of this image are shown in Fig. 2

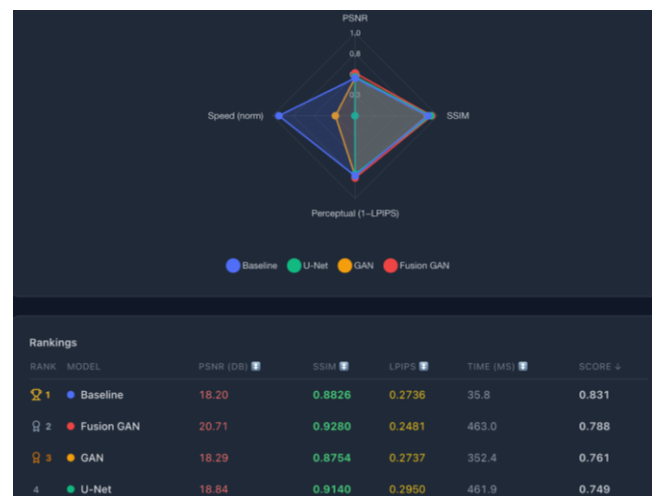


Fig. 2. Numerical results of the colorization of single image

Visual analysis revealed characteristic patterns in the performance of each architecture type.

Basic CNN demonstrates (see Fig. 3) the most uniform but washed-out results. In complex areas, a pronounced brown or gray tint often appears, making the image look unnatural.

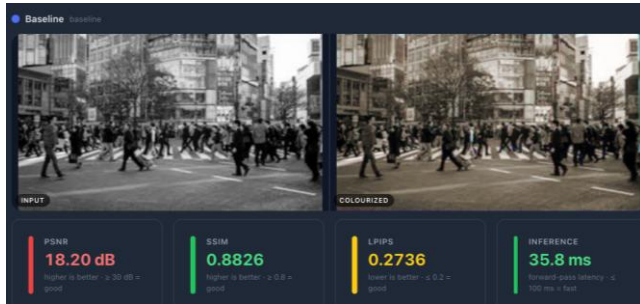


Fig. 3. Colorization result with Baseline CNN model

U-Net demonstrates (see Fig. 4) high structural accuracy. The model handled basic colors well – blue skies, green grass, and natural skin tones. However, on large monochromatic areas, it remains too conservative, avoiding saturated colors.

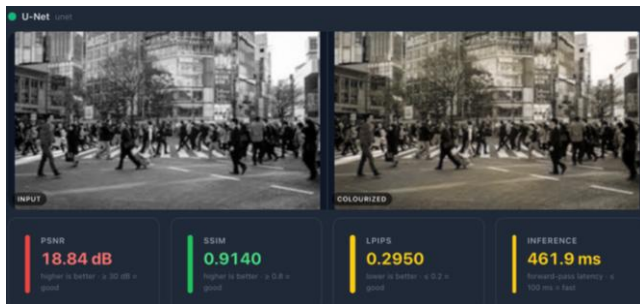


Fig. 4. Colorization result with U-Net model

cGAN provides (see Fig. 5) the highest color diversity at the local level. The network excellently reproduces vivid details – flowers, patterns on clothing, and the play of light. However, global artifacts sometimes appear in background areas where color may be distributed unevenly.

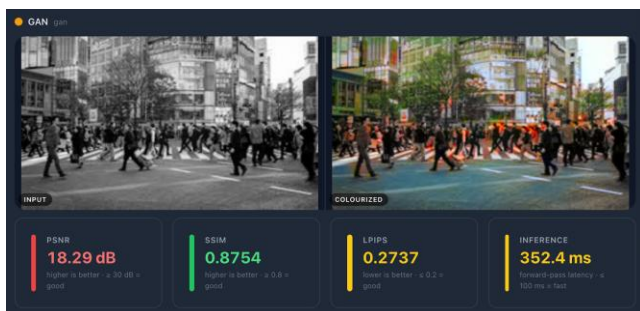


Fig. 5. Colorization result with cGAN model

Fusion GAN (see Fig. 6) appears to be the most balanced in scenes with a clear narrative. It retains the vibrancy of generative adversarial networks but adds logical coherence. At the same time, in very complex compositions with many objects, minor color inaccuracies characteristic of GAN models may still remain.

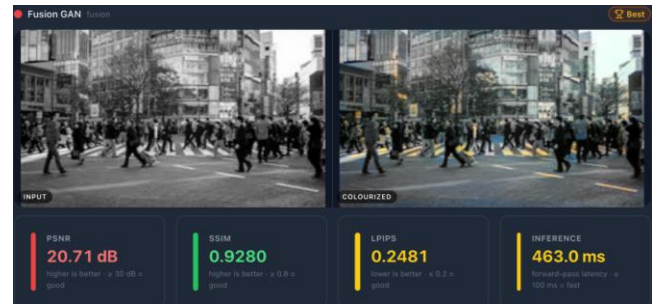


Fig. 6. Colorization result with Fusion GAN model

V. CONCLUSIONS

A. Why Does U-Net Lead in the Numbers?

The high performance of the U-Net architecture requires careful interpretation. Traditional metrics, such as PSNR and SSIM, penalize the model for any deviation from the original, even if the result looks natural to the human eye [13]. Since U-Net makes “conservative” predictions close to the dataset’s mean values, it automatically incurs fewer penalties for distortion.

However, the fact that even the LPIPS metric favors this architecture indicates the great importance of structural accuracy. On diverse datasets (such as the COCO dataset), where there is no single dominant color theme, strict adherence to object boundaries proves to be a more significant factor for perception than high saturation. Our findings align with the results of other COCO-based studies: under limited training time, U-Net-style architectures consistently outperform simpler models across all metrics.

B. The Trade-off Between Mathematical Accuracy and Realism

We found a direct correlation between loss functions and the quality of the final image. Using L2 regression inevitably leads to desaturation – the image becomes dull and grayish [5]. The L1 function somewhat corrects this effect, but true color diversity is restored only by a combination of adversarial loss and VGG-16 perceptual features [14].

At the same time, this approach introduces an element of unpredictability, which degrades technical accuracy metrics at the level of individual pixels. This fundamental trade-off – between pixel-perfect alignment and visual realism – confirms that no single metric can provide the full picture. This is precisely why the combined PSNR/SSIM/LPIPS system is indispensable for comparative studies in the field of colorization.

C. Study Limitations

Our findings have three important limitations. First, a training budget of 20 epochs and a sample of 2,000 images are rather restrictive conditions for GAN models. Such architectures typically require significantly more iterations to fully realize their potential. Second, we did not involve real people in the evaluation (e.g., through “deception level” tests); no automatic algorithm is yet capable of 100% replacing the human eye, especially when it comes to the

results of competitive training [5]. Third, all experiments were conducted at a fixed resolution of 256×256 . The performance of models on large images, where understanding the overall context of the scene becomes even more critical, requires separate investigation.

D. Directions for Further Research

Our results open up several promising avenues for the future development of this topic:

- **Scaling up training.** Increasing the training duration (beyond 100 epochs) on the full COCO 2017 dataset. This will allow GAN-based models to fully realize their qualitative potential, which is currently hindered by time constraints.
- **Global analysis based on Transformers (ViT).** If we replace ResNet-18 in our Fusion GAN model with the Vision Transformer architecture, the system will be able to understand the complex context of a scene much better. This will solve the “myopia” problem of the local PatchGAN, which has already been demonstrated using the DDColor model [9].
- **Improved Initialization.** Extending the biologically motivated weight initialization strategy [12] to all network components. This will make training even deeper architectures more stable and reduce the risk of getting stuck during training.
- **Human evaluation.** Introduction of “authenticity vs. forgery” (AMT) tests. Since no automatic formulas can fully replace human perception, this approach will help evaluate the realism of generated GAN images more objectively [13].
- **Application of diffusion models.** Using our global cue vector together with latent diffusion models (LDM). This could be the key to achieving truly photorealistic quality while maintaining acceptable processing speed.

E. General Conclusions

In this paper, we conducted a comprehensive and systematic comparison of four neural network architectures for colorizing monochrome images based on the COCO 2017 dataset. The results fully confirmed theoretical expectations. The baseline CNN clearly demonstrated that the use of L2 regression inevitably leads to color averaging and causes an undesirable “sepia effect” [5].

In contrast, U-Net [6] proved to be the most effective tool under conditions of limited training time. Thanks to its cross-connections and L1 loss function, this architecture successfully combines high structural accuracy with an acceptable level of realism and excellent speed (approximately 118 ms per image). The stability of such deep networks is further supported by proper biologically motivated weight initialization [12].

Generative adversarial networks (cGANs) [7] have demonstrated the ability to generate vivid and rich textures; however, due to the local focus of the PatchGAN discriminator, they often made semantic errors across the entire scene. Our Fusion GAN modification successfully

mitigated this issue: integrating global cues from ResNet-18 [10] significantly improved contextual integrity in scenes with a clear narrative. It is worth noting that this multi-branch data fusion approach has also proven effective in other critical computer vision systems, such as road hazard detection [15].

The study also confirmed that a comprehensive system of PSNR/SSIM/LPIPS metrics [13] is indispensable for an objective evaluation of colorization. No single metric alone is capable of revealing all the trade-offs that models make during generation.

Ultimately, our work demonstrates that a relatively simple architecture with properly configured feed-through connections and loss functions remains an extremely powerful solution for practical tasks. At the same time, we have established a clear direction for future research that will help finally bridge the gap between mathematical accuracy and visual realism. And our specially developed web platform [2], which ensures reliable data input and processing, makes this process convenient and fully reproducible for any future experiments.

REFERENCES

- [1] S. Anwar, M. Tahir, C. Li, A. Mian, F. S. Khan, and A. W. Muzaffar, “Deep Learning for Image Colorization: A Survey,” arXiv preprint arXiv:2008.10774, 2024. [Online]. Available: <https://arxiv.org/abs/2008.10774>. DOI: <https://doi.org/10.48550/arXiv.2008.10774>
- [2] S. Bielevietsov, I. Ruban, K. Smelyakov, and D. Sumtsov, “Network technology for transmission of visual information,” in Selected Papers of the XVIII Int. Sci.-Practical Conf. “Information Technologies and Security” (ITS 2018), Kyiv, Ukraine, Nov. 27, 2018, CEUR Workshop Proceedings, vol. 2318, 2018, pp. 160–175. [Online]. Available: <https://ceur-ws.org/Vol-2318/>
- [3] T. Welsh, M. Ashikhmin, and K. Mueller, “Transferring Color to Greyscale Images,” ACM Trans. Graph. (Proc. SIGGRAPH), vol. 21, no. 3, pp. 277–280, 2002. DOI: <https://doi.org/10.1145/566654.566576>
- [4] A. Levin, D. Lischinski, and Y. Weiss, “Colorization Using Optimization,” ACM Trans. Graph. (Proc. SIGGRAPH), vol. 23, no. 3, pp. 689–694, 2004. DOI: <https://doi.org/10.1145/1186562.1015780>
- [5] R. Zhang, P. Isola, and A. A. Efros, “Colorful Image Colorization,” in Proc. European Conf. Computer Vision (ECCV), Amsterdam, Netherlands, 2016, pp. 649–666. DOI: <https://doi.org/10.48550/arXiv.1603.08511>
- [6] O. Ronneberger, P. Fischer, and T. Brox, “U-Net: Convolutional Networks for Biomedical Image Segmentation,” in Proc. Int. Conf. Medical Image Computing and Computer-Assisted Intervention (MICCAI), Munich, Germany, 2015, pp. 234–241. DOI: <https://doi.org/10.48550/arXiv.1505.04597>
- [7] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, “Image-to-Image Translation with Conditional Adversarial Networks,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017, pp. 1125–1134. DOI: <https://doi.org/10.48550/arXiv.1611.07004>
- [8] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative Adversarial Nets,” in Advances in Neural Information Processing Systems (NeurIPS), vol. 27, 2014. DOI: <https://doi.org/10.48550/arXiv.1406.2661>
- [9] X. Kang, T. Yang, W. Ouyang, P. Ren, L. Li, and X. Xie, “DDColor: Towards Photo-Realistic Image Colorization via Dual Decoders,” in Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV), Paris, France, 2023, pp. 328–338. DOI: <https://doi.org/10.48550/arXiv.2212.11613>

- [10] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, pp. 770–778. DOI: <https://doi.org/10.1109/CVPR.2016.90>
- [11] S. Iizuka, E. Simo-Serra, and H. Ishikawa, "Let there be Color!: Joint End-to-end Learning of Global and Local Image Priors for Automatic Image Colorization with Simultaneous Classification," ACM Trans. Graph. (Proc. SIGGRAPH), vol. 35, no. 4, pp. 110:1–110:11, 2016. DOI: <https://doi.org/10.1145/2897824.2925974>
- [12] O. Zolotukhin, Y. Bodyanskiy, V. Filatov, M. Kudryavtseva, and Y. Yermieiev, "Stochastic Initialization for Neural Networks Based on the Analysis of Biological Systems," in Proc. 5th Int. Workshop of IT-Professionals on Artificial Intelligence (ProFIT AI 2025), Liverpool, United Kingdom, Oct. 15–17, 2025, pp. 415–426. [Online]. Available: <https://ceur-ws.org/Vol-4164/>
- [13] R. Zhang, P. Isola, A. A. Efros, E. Shechtman, and O. Wang, "The Unreasonable Effectiveness of Deep Features as a Perceptual Metric," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Salt Lake City, UT, USA, 2018, pp. 586–595. DOI: <https://doi.org/10.1109/CVPR.2018.00068>
- [14] J. Johnson, A. Alahi, and L. Fei-Fei, "Perceptual Losses for Real-Time Style Transfer and Super-Resolution," in Proc. European Conf. Computer Vision (ECCV), Amsterdam, Netherlands, 2016, pp. 694–711, DOI: https://doi.org/10.1007/978-3-319-46475-6_43
- [15] O. Byzkrovnyi, L. Savulioniene, K. Smelyakov, P. Sakalys, and A. Chupryna, "Comparison of Potential Road Accident Detection Algorithms for Modern Machine Vision System," Vide. Tehnologija. Resursi – Environment, Technology, Resources, vol. 3, pp. 50–55, 2023. DOI: <https://doi.org/10.17770/etr2023vol3.7299>

University Libraries in the Digital Ecosystem of Cultural Memory and Strategies for Digitization, Access, and Knowledge Sharing

Trayana Petrova
Library and Information Center
University of Library Studies and
Information Technologies
Sofia, Bulgaria
t.velkova@unibit.bg

Panayot Gindev
Information Systems and
Technologies Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
p.gindev@unibit.bg

Iliyana Kamburova
Library and Information Center
University of Library Studies and
Information Technologies
Sofia, Bulgaria
i.kamburova@unibit.bg

Abstract—Preserving and providing access to documentary cultural heritage poses a significant challenge in the context of today's digital transformation. The development of information technologies creates new opportunities for the digitization, preservation, and dissemination of archival and library resources, as well as for expanding access to knowledge. University libraries play a vital role in building the digital ecosystem of cultural memory by supporting the processes of digitization, management, and provision of access to information resources. By implementing modern technologies and developing institutional collaboration, they contribute to the more effective preservation and promotion of documentary heritage. This publication explores opportunities for developing strategies for the digitization and management of information resources in university libraries, as well as the importance of cooperation among various cultural memory institutions. The focus is on the role of university libraries as intermediaries in the processes of knowledge exchange and ensuring broader access to cultural heritage in a digital environment.

Keywords— *cultural memory, digitization, university libraries, documentary cultural heritage, information resources.*

I. INTRODUCTION

Documentary cultural heritage is a key element of a country's identity and is essential to its development. By utilizing the latest technologies, we can ensure that it is preserved for future generations and remains accessible to people at any time and from any location [1], [2], [3].

The preservation and protection of documentary cultural heritage is a challenge not only for institutions but also for library staff, as they bear the responsibility for its preservation. This study focuses on the nature,

applicability, and significance of preserving community center collections, as well as new opportunities for inter-institutional cooperation, research, and engaging local communities in cultural sustainability processes by incorporating digital technologies as a tool for preserving and accessing documentary heritage, in accordance with established best practices and professional standards [4], [5].

A good opportunity for the preservation of library collections is the creation of digital collections that are available to users at any time, without restrictions [2], [3], [6]. The benefits of digitization include the possibility of broader and easier access to documents and the preservation of original editions. This is a way to properly assess the value and significance of the collections held [3], [5], [7].

Digitizing the collections will preserve them over time, and regardless of the extent of their deterioration, their digital images will always be available to future generations. In addition to the benefits of preservation and conservation, digitization also benefits users by providing them with convenient and fast access to information [3], [8].

Despite the growing number of digitization initiatives, the development of models that link the capacity of university libraries with the needs of smaller memory institutions at the regional level remains relatively limited in the scientific literature. It is precisely here that the need for networked solutions becomes apparent, in which the university library functions not only as an independent service provider but also as a coordinating center for digitization, methodological, and training activities. This publication aims to argue for the applicability of such a model and to outline its main functional components in an

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.93>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

environment where the sustainability of digital resources depends simultaneously on technology, organizational policies, and human capacity [9], [10], [11].

In this regard, the study is guided by three main questions: what are the institutional and technological prerequisites for building sustainable digital services; how can university libraries support community and regional collections, and which mechanisms for describing, sharing, and visualizing digital objects are most suitable for creating a shared access infrastructure? Formulating these questions allows the topic to be viewed not merely as a digitization task, but as a challenge concerning the management of cultural memory, information connectivity, and the public visibility of local cultural resources [1], [2], [3].

II. RESEARCH METHODOLOGY

A. Research Framework and Analysis Criteria

The study is conceptual and analytical in nature and employs a qualitative approach based on a comparative review of international strategic documents, publications in the field of digital libraries, and research dedicated to the digital preservation of cultural heritage. The analysis includes documents from UNESCO and IFLA, publications addressing digitization as part of cultural heritage management, as well as European frameworks related to integrated platforms and shared services in the sector [1], [2], [3], [12], [10], [11].

For the purposes of this study, five analytical criteria have been identified:

- a) institutional organization and partnership;
- b) selection and prioritization of items for digitization;
- c) description, metadata, and interoperability;
- d) long-term preservation and access;
- e) human resource development and service sustainability.

Through this framework, the proposed model for a digitization hub is viewed as a managerial and technological construct, rather than merely a technical process of scanning and publishing files. Such an analytical approach allows for an assessment of the relationships between the quality of digital resources, their reusability, and their actual integration into educational, scientific, and public practice [9], [10], [11].

The intensive digital transformation, the sustainable preservation, and access to documentary heritage are becoming increasingly important, both for the scientific community and for the general public. In this context, libraries—and in particular university and community libraries—are establishing themselves as key institutions in the process of preserving, digitizing, and promoting documentary heritage [3], [9].

Issues related to the preservation of archival collections are of particular importance for small communities, where

valuable but poorly accessible or at-risk documents are stored in community center libraries [5], [12].

Community centers are a unique institution within the Bulgarian cultural system. They play a vital role in preserving and promoting local culture, traditions, and historical memory. Their collections contain valuable documents related to regional history, cultural events, and community life [5].

The digitization of documentary cultural heritage is a strategic task for modern libraries and cultural institutions. However, serious difficulties are encountered in implementing such initiatives due to limited resources and a lack of technical infrastructure [8], [12].

The main problems include limited financial resources, a lack of technical infrastructure, and insufficiently trained staff. As a result, a significant portion of the local documentary cultural heritage remains inaccessible to the general public and to scientific research [8], [12].

In this context, collaboration between university libraries and local cultural institutions can be viewed as an effective model for developing digital services. University libraries possess technological resources, expertise, and organizational capacity that can be leveraged to support smaller institutions. For these reasons, the creation of collaborative networks between different institutions is viewed as an effective approach for developing digital initiatives in the cultural sector [10], [11].

The proposed model for a digitization hub provides an opportunity for effective collaboration between university libraries and community centers. Through centralized infrastructure and resource sharing, the digitization process can be improved and broader access to documentary cultural heritage can be ensured. The digitized resources will be consolidated into a platform to facilitate the sharing of and access to information among participating institutions [10], [11].

In all programs for the preservation of and access to the cultural heritage of libraries, a role is assigned to educational, cultural, and social institutions that provide free and open access to information. All these changes require continuous maintenance of specific software resources and a secure technical infrastructure, as well as ongoing training for staff [12], [11], [13].

Today, the library has established itself not only as a repository of knowledge, but also as a facilitator in the development of an informed, critically thinking, and culturally aware society. The university library is a cultural, educational, social, and information hub capable of responding flexibly and appropriately to the challenges of the modern era. This transformation is of essential importance for contemporary higher education institutions, establishing the university library as an indispensable resource and partner in building a sustainable and innovative academic community [9], [14].

III. RESULTS

A. Interoperability and Metadata

One of the key findings of the analysis is that the proposed model for a digitization hub must be built on a common minimum set of requirements for metadata, file formats, and information exchange procedures. Dublin Core can be used for basic bibliographic and descriptive representation, as it provides a widely recognized set of elements for describing digital resources and facilitates comparability between different systems [15]. When the hub aims to exchange metadata between institutional repositories, library catalogs, and external aggregators, a suitable mechanism is OAI-PMH, which allows for the retrieval and reuse of structured descriptions from various sources [16]. For the online presentation of complex digital objects such as manuscripts, periodicals, albums, and multi-page documents, IIIF provides the necessary framework for visualization, navigation, and annotation, without requiring each institution to build its own completely closed-off toolkit [17].

It follows, then, that the quality of digitization is not determined solely by image resolution, but by the system's overall ability to ensure discoverability, link descriptive and visual data, and enable the resource to be used across multiple platforms. It is precisely at this level that the university library can act as a methodological coordinator, establishing minimum requirements for metadata, file formats, identifiers, naming conventions, and quality control procedures [9], [10], [15], [16], [17].

B. Model for Institutional Partnership

The results of the comparative analysis show that the phased model of cooperation is the most promising. In the first phase, partner institutions identify and prioritize locally significant documents. In the second stage, the university library provides digitization methodologies, training, technical consultations, and basic storage infrastructure. In the third stage, centralized cataloging and publication in a shared access environment are implemented, and in the fourth stage, integration with national and international platforms to increase the resource's visibility. This model reduces inequalities between institutions with varying capacities while simultaneously creating conditions for the accumulation of shared expertise [8], [10], [11].

In such an architecture, community libraries retain their role as custodians of local memory and providers of primary materials, while university libraries assume more pronounced coordinating and scientific-information functions. This division of roles is important because it prevents both over-centralization and the fragmented development of separate, incompatible initiatives. In practice, the digitization hub should combine technical infrastructure, editorial policy, copyright rules, archiving procedures, and channels for promoting digital collections [2], [12], [11], [18].

C. Access, Reuse, and Public Value

Ensuring access should not be limited solely to the online publication of images or PDF files. European best practices show that the real public value of digital collections increases when they are accompanied by high-quality metadata, clear licensing terms, and the ability to cite and incorporate them into educational, research, and creative uses [11], [18]. In this sense, access is a multifaceted process that encompasses discoverability, understandability, reusability, and thematic linking to other resources.

For university libraries, this means developing services that go beyond traditional bibliographic reference: creating thematic digital collections, curated virtual exhibitions, information literacy training resources, and research services for working with digitized sources. When local cultural resources are presented in such an expanded environment, they transform from obscure archival items into active objects of research, teaching, and cultural communication. In this way, digitization supports not only the preservation but also the revitalization of cultural memory in the contemporary digital environment [3], [9], [14].

D. Sustainability and Human Resource Capacity

A key finding of the analysis is that the sustainability of such initiatives depends equally on technology and human resources. The availability of scanners, a server environment, and an access platform is a necessary but insufficient condition if clear workflows, responsibilities, and competencies are lacking. Training is needed in digitization, metadata, copyright, file management, quality control, and the basic principles of digital preservation. It is precisely here that university libraries can serve as training centers for regional partners and create sustainable communities of practice [8], [8], [10].

Sustainability also requires a clear policy on technological upgrades, backups, long-term storage formats, and periodic verification of available digital resources. Otherwise, the risk shifts from physical damage to the original to digital obsolescence, file fragmentation, and loss of descriptive information. Therefore, the digital hub should be conceived as an ongoing organizational process rather than a one-time project dependent solely on short-term funding [1], [12], [11].

E. Stages of Digital Curation

The practical implementation of the proposed model requires a clearly defined workflow that begins with the selection and assessment of the physical condition of the documents, proceeds through digital capture, the creation of master files, the production of derivative copies for access, metadata description, quality control, and publication in a search and visualization environment. The inclusion of standardized descriptive elements and clearly defined stages reduces the risk of inconsistent processing and facilitates the subsequent sharing of resources between institutions [12], [15], [17]. Such a workflow is particularly important in distributed partner networks, where digital objects are created in different locations but must be

presented in a consistent manner and with predictable quality.

It is particularly important to distinguish between files intended for long-term preservation and those intended for public access. The former should be designed to maintain the highest possible quality and ensure the possibility of future migration, while the latter must provide fast loading, convenient viewing, and controlled use in a web environment. When this distinction is not taken into account, the result is often either excessively large public collections or a lack of sufficiently reliable source files for future reuse and long-term preservation. This is why quality control must be conceived as an ongoing function of the hub, rather than as a final, one-time check [12], [11], [18].

F. Policies, Rights, and Ethical Considerations

The digitization of documentary cultural heritage also involves a number of decisions regarding copyright status, the provenance of materials, the degree of public access, and permissible forms of reuse. Not all items can or should be published in the same way. Some documents may contain sensitive data, restrictions arising from third-party rights, or special social and local significance that requires more careful curation. Therefore, an effective digitization hub must have transparent rules regarding rights, licenses, and access levels so as to balance openness with institutional accountability [1], [2], [11], [18].

Aligning domestic policies with European frameworks for quality and reuse also has practical significance. It facilitates not only publication within broader ecosystems but also builds trust in digital collections as a reliable scientific and educational resource. When sufficient descriptive data, clear rights, and a stable access address are added to each digital object, the likelihood that it will be cited, used in teaching, or included in broader thematic collections increases significantly. In this way, access and rights policies become an essential element of the visibility and lifecycle of digital heritage [10], [11], [18].

IV. CONCLUSION

The development of such network models can contribute to the creation of sustainable digital ecosystems that support scientific research, education, and cultural development.

Access to information plays a vital role in today's information-based society. Therefore, university libraries must ensure both every user's right to equal access to information and the necessary means for its effective realization, while encouraging the search for and use of information. University libraries are among the most important venues for accessing and sharing information. To fulfill their mission effectively and serve their users well, they must have qualified staff, a solid technical infrastructure, and support from the institutions themselves. Only then will they be able to adequately meet the needs of their users and develop the services they offer.

In this sense, the proposed model makes a twofold contribution: first, it formulates a practical framework for

cooperation between university libraries and community centers; second, it emphasizes interoperability, metadata quality, and access policies as essential dimensions of modern digitization. It is particularly important that such a framework can be adapted to the scale and resources of the participating institutions without losing the possibility of subsequent integration with broader European ecosystems.

A limitation of this study is its conceptual nature—it does not include empirical testing of the model within a specific institutional network. This opens up prospects for future work focused on piloting the proposed framework, developing indicators for quality assessment, and tracking the impact of digital collections on scholarly use, educational practices, and the public visibility of local cultural heritage. Regardless, the analysis shows that university libraries have the potential to be not only custodians of knowledge but also active architects of a connected and shared digital cultural memory.

From a practical standpoint, the implementation of such a model can be carried out in stages: first by establishing a minimal set of standards for metadata description and exchange, then by creating a common access portal, and finally by linking local digital collections to national and international aggregators. This phased approach allows institutions to increase their capacity without disrupting their current operations and without making the entire sustainability of the initiative dependent on a one-time project resource. This is precisely why the combination of phased implementation, interoperability, and clear digital curation policies appears most suitable for university libraries that wish to take on a coordinating role in the preservation and promotion of local cultural heritage.

ACKNOWLEDGMENTS

This publication was produced as part of the research project „Digital Hub for Cultural Memory: An Academic Model for the Digitization and Access to Library and Community Center Resources,” under contract No. KP-06-M100/2 dated December 10, 2025, funded by the Scientific Research Fund of the Ministry of Education and Science, Republic of Bulgaria.

REFERENCES

- [1] UNESCO, “Charter on the Preservation of the Digital Heritage,” Paris, France, Oct. 15, 2003. [Online]. Available: <https://unesdoc.unesco.org/ark:/48223/pf0000229034>. [Accessed: Apr. 24, 2026].
- [2] International Federation of Library Associations and Institutions (IFLA), “IFLA/UNESCO Manifesto for Digital Libraries,” 2011. [Online]. Available: <https://repository.ifla.org/handle/20.500.14598/3583>. [Accessed: Apr. 24, 2026].
- [3] C. Lynch, “Digital Collections, Digital Libraries and the Digitization of Cultural Heritage Information,” *First Monday*, vol. 7, no. 5, May 2002, doi: 10.5210/fm.v7i5.949.
- [4] D. Pavlova, I. Peteva, and I. Pavlova, “Cultural Heritage through the Lens of e-Governance,” *Digital Presentation and Preservation of Cultural and Scientific Heritage*, vol. 13, pp. 311–316, 2023, doi: 10.55630/dipp.2023.13.32.
- [5] K. Ivanova and K. Zdravkov, “Digital Collections in Regional Public Library ‘P. R. Slaveikov’ – Veliko Tarnovo in the Context of the National Program for Preservation and Promotion of

- Literary Heritage,” *Digital Presentation and Preservation of Cultural and Scientific Heritage*, vol. 1, p. 180, 2011, doi: 10.55630/dipp.2011.1.22.
- [6] T. M. Masenya and P. Ngulube, “Digital preservation practices in academic libraries in South Africa in the wake of the digital revolution,” *South African Journal of Information Management*, vol. 21, no. 1, a1011, 2019, doi: 10.4102/sajim.v21i1.1011.
- [7] European Commission, Directorate-General for Communications Networks, Content and Technology, *Europeana Strategy 2020–2025: Empowering Digital Change*. Luxembourg: Publications Office of the European Union, 2020, doi: 10.2759/524581T. M. Masenya and P. Ngulube, “Digital preservation practices in academic libraries in South Africa in the wake of the digital revolution,” *South African Journal of Information Management*, vol. 21, no. 1, a1011, 2019, doi: 10.4102/sajim.v21i1.1011.
- [8] Dublin Core Metadata Initiative, “DCMI Metadata Terms,” Jan. 20, 2020. [Online]. Available: <https://www.dublincore.org/specifications/dublin-core/dcmi-terms/2020-01-20/>. [Accessed: Apr. 24, 2026].
- [9] European Commission, Directorate-General for Research and Innovation, P. Brunet et al., *Report on a European Collaborative Cloud for Cultural Heritage: Ex-ante Impact Assessment*. Luxembourg: Publications Office of the European Union, 2022, doi: 10.2777/64014.
- [10] I. S. Sverrisdóttir, K. Sigurðsson, and Ö. Hrafnkelsson, “Access and Curation of Digital Cultural Heritage in the National and University Library of Iceland,” *Microform & Digitization Review*, vol. 41, nos. 3–4, pp. 97–102, 2012, doi: 10.1515/mir-2012-0014.
- [11] IIIF Consortium, “Presentation API 3.0,” 2020. [Online]. Available: <https://iiif.io/api/presentation/3.0/>. [Accessed: Apr. 24, 2026].
- [12] Europeana Foundation, “Europeana Publishing Framework: Content,” 2018. [Online]. Available: https://pro.europeana.eu/files/Europeana_Professional/Publications/Publishing_Framework/Europeana_publishing_framework_content.pdf. [Accessed: Apr. 24, 2026].
- [13] K. Nusheva, “Digitalizatsiyata kato sredstvo za opazvane na bibliotechnite koleksii” [Digitalization as a Means of Preserving Library Collections], *Knigata – nasheto po-smisleno nastoyashte*, no. 2, pp. 214–220, 2012.
- [14] K. Mincheva, “Transformatsii ‘Biblioteka – bibliotечen media tsentar’ – funktsionalni modeli i dobri bibliotечni praktiki” [Library Transformation into Media Centers – Functional Models and Good Practices], in *Libraries, Reading, Communications: Ninth National Scientific Conference with International Participation*, Veliko Tarnovo, Bulgaria, 2011, pp. 322–331.
- [15] E. Savova, D. Stoyanova, and T. Petrova, “The Institutions of Memory – the Modern Educational Environment,” *Education, Scientific Research and Innovations*, vol. I, issue 2, pp. 39–45, 2023, doi: 10.70300/MJNA8201. [Online]. Available: https://e-journal.unibit.bg/images/proceedings/2023/book2/Statiq_4_Elena_Savova_D_Stoqnova_T_Petrova.pdf. [Accessed: Apr. 24, 2026].
- [16] B. de la Porte and R. Higgs, “Challenges in digitisation of cultural heritage material in the Western Cape, South Africa,” *South African Journal of Information Management*, vol. 21, no. 1, a1104, 2019, doi: 10.4102/sajim.v21i1.1104.
- [17] C. L. Liew, “Towards dynamic and evolving digital libraries,” *The Electronic Library*, vol. 32, no. 1, pp. 2–16, 2014, doi: 10.1108/EL-07-2012-0089.
- [18] Open Archives Initiative, “The Open Archives Initiative Protocol for Metadata Harvesting,” ver. 2.0, Jun. 14, 2002. [Online]. Available: <https://www.openarchives.org/OAI/openarchivesprotocol.html>.

Ground Operational Picture Improvement Through Direct Georeferencing from an Unmanned Aerial System

Venelin Rashkov

Communication and Information
Systems Directorate
Ministry of Defence
Sofia, Bulgaria
v.rashkov@mod.bg

Alexander Kolev

Development of C4I
Systems Directorate
Defence Institute
"Prof. Tsvetan Lazarov"
Sofia, Bulgaria
a.kolev@di.mod.bg

Abstract - This paper presents an approach to improving the ground operational picture by applying direct georeferencing techniques from an unmanned aerial system (UAS). The study addresses the growing need for rapid and accurate target localization within time-critical operational environments, where minimizing latency and maximizing spatial accuracy are essential.

The proposed methodology leverages onboard GNSS/INS data and calibrated imaging sensors to assist in determining the geospatial coordinates of observed objects without reliance on ground control points. A transformation model based on intrinsic and extrinsic camera parameters is implemented to ensure precise mapping between image space and object space.

The integration of direct georeferencing into the target management cycle significantly reduces processing time compared to conventional indirect methods. Experimental results indicate improved time performance and, consequently, enhanced operational efficiency, particularly in dynamic and data-intensive scenarios such as surveillance and reconnaissance missions.

The proposed approach supports near real-time performance and provides a scalable solution for advanced UAS-based targeting systems.

Keywords — *Direct Georeferencing; GNSS/INS Integration; Real-Time Geospatial Processing, Unmanned Aerial Systems (UAS).*

I. INTRODUCTION

In modern operational environments, particularly in military, security, and emergency response contexts, the ground operational picture (GOP) represents the real-time or near-real-time understanding of the situation on the ground. This includes the location, identification, and tracking of targets, assets, and threats [1]. Traditional methods for building and updating the GOP often rely on

indirect georeferencing techniques that require extensive post-processing, ground control points (GCPs), or manual intervention. While these methods provide high accuracy, they are time-consuming and unsuitable for time-critical missions. In dynamic operational environments, the delay between data acquisition and actionable intelligence can significantly impact mission success. Conventional workflows involve multiple stages of data processing, including image triangulation and adjustment, which introduce latency.

The rapid development of Unmanned Aerial Systems (UAS) has significantly transformed modern surveillance, reconnaissance, and targeting operations. UAS, commonly known as drones, have emerged as powerful platforms for aerial reconnaissance and surveillance due to their flexibility, low operational cost, and ability to operate in contested or inaccessible areas [2], [3]. However, the full potential of UAS-derived imagery is realized only when the collected data can be accurately and rapidly georeferenced to real-world coordinates.

Direct georeferencing offers a compelling solution by determining the geospatial position and orientation of the imaging sensor directly from onboard navigation systems (GNSS/INS) without the need for GCPs or complex aerial triangulation. This approach minimizes latency, reduces dependency on ground infrastructure, and enables faster integration of imagery into command-and-control systems.

This paper explores the application of direct georeferencing from a UAS to enhance the GOP. We present a methodology that integrates calibrated camera parameters with high-precision onboard navigation data, implement a collinearity-based transformation model, and evaluate its performance in terms of accuracy and processing time. The results demonstrate significant

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.101>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

improvements in operational efficiency for surveillance and reconnaissance missions.

II. MATERIALS

The georeferencing procedure has been used extensively not only for updating but also creating digital GIS data. Specialized software products are known where a desirable effect is achieved with the intervention of a human operator and by following a certain sequence of actions. The necessity of instantly updatable digital geographic data demands greater automation of the georeferencing process.

One of the approaches for automated georeferencing is presented in the publication [4]. The authors Xiangyu Zhuo at all are proposing to apply Image Processing methods in the georeferencing of a photo image captured by an Unmanned Aerial Vehicle (UAV) onto previously georeferenced by various techniques single objects that are expected to be included in the field of view of the capturing camera. The authors have declared the achievement of sufficiently high accuracy. Thus, the proposed approach would have a more limited application when the image to be georeferenced is captured at an incorrect angle, and is inapplicable when some of the fixed objects with known coordinates are not in the frame.

A universal approach called "direct georeferencing" is represented in the publication [5]. The authors of the material Carlos A. M. Correia at all consider a mathematical computational approach where the input data from the UAV's on-board sensors, the Global Positioning System (GPS) receiver and the Inertial Measurement Unit (IMU) are implemented in a way that given pixels of the captured image can be correlated with real geographical coordinates of the captured terrain. Computation simulation results using the specialized software MATLAB, Unreal Engine 4 and AirSim are described. A practical experiment with the Robot Operating System shows the applicability of the direct georeferencing method. The optimal choice of the used mathematical technique and the estimation of the error resulting from the inherent uncertainties in the readings of the on-board sensors remain a matter of discussion.

Materials [6], [7] are focused on real-time monitoring of natural disasters, such as fire, volcano, flood, landslide, and coastal inundation, highly-accurate georeferenced remotely sensed imagery is needed. Georeferenced imagery can be fused with geographic spatial data sets to provide geographic coordinates and positing for regions of interest. In this paper authors proposes an on-board georeferencing method for remotely sensed imagery, which contains five modules: input data, coordinate transformation, bilinear interpolation, and output data. The experimental results demonstrate multiple benefits of the proposed method.

There is a well-known mode Real-Time Kinematic (RTK). This mode of automated image processing is designed for fast, near-real-time georeferencing with the highest possible accuracy. As a rule, a satellite navigation reference system is used, employing reference ground

stations from the national network or proprietary, specialized GPS devices designed for this purpose. In addition to the geographic coordinates at the time of capture, the current spatial position data of the optical axis of the camera lens are also recorded. In commercially available RTK photo-video devices, the subsystem is independent of the rest of the onboard equipment and has its own precise GPS and IMU. Georeferencing data is recorded in the metadata section of the image file, typically using the Exchangeable Image File Format (EXIF) [6]. In the same EXIF format, characteristic parameters of the photo-electronic system, such as resolution, optical sensor dimensions, pixel size, focal length, field of view, and exposure time, are also recorded in the image metadata. The images prepared in this way are transmitted to the Ground Control Station (GCS) via a digital wireless data link, or downloaded to an electronic storage media after the aircraft lands.

As discussed in the materials previously cited, the direct georeferencing approach is appropriate when there is a need to rapidly acquire up-to-date georeferenced digital mapping information. In order to establish the usefulness of the practical application of such an approach in this paper, the authors propose mathematical apparatus, experimental environment and field-testing results of a practical use of the Automatic Direct Georeferencing approach.

III. METHODS

A. Georeferencing a raster image

The raster image obtained by the drone camera is considered as a collection of its smallest constituent unit - pixels (picture elements) arranged in a matrix. The arrangement of the pixels in the matrix depends on their position (row and column) in the digital image. The amount of pixels determines the resolution of the image, expressed in number of pixels in width and height. Unlike mathematical coordinate systems, the origin of the coordinate system of the pixels in the image (0,0) is the upper left corner [8], [9].

Georeferencing a raster image superimposed on a map rendered as a vector graphic (vector map), we need to determine the correction coefficients. The purpose of the correction coefficients is to ensure that each pixel of the image corresponds as closely as possible to the actual ground coordinates of the vector map. The applicable system of correction coefficients depends on the chosen transformation model. Transformation models can be of several types which generally perform translation, rotation, scaling and shearing.

One basic and commonly used transformation model is the affine transformation, which has a mathematical representation as a first-order polynomial.

$$x_i = a_0 + a_1X_i + a_2Y_i \quad (1)$$

$$y_i = b_0 + b_1X_i + b_2Y_i \quad (2)$$

where:

$P\{X_i, Y_i\}$ – coordinates (column, row) of pixels in the image matrix, starting from the upper left corner;

$L\{x_i, y_i\}$ – coordinates (in metric coordinate system) of Ground Control Points in the terrestrial coordinate system that correspond to $\{x_i, y_i\}$;

a_1 is pixel size in x-direction;

b_1 is rotation about y-axis;

a_2 is rotation about x-axis;

b_2 is pixel size in y-direction;

a_0 is x-coordinate of center of the upper left pixel;

b_0 is y- coordinate of center of the upper left pixel;

$i = 0 \dots N-1, N \geq 3$ (the number of GCPs required is at least 3 when working with a first order polynomial).

When certain values of $P\{X_i, Y_i\}$ and $L\{x_i, y_i\}$ are known, the values of the coefficients a and b must be determined in order to perform the coordinate transformation.

Equations (1) and (2) could also be described mathematically in matrix form:

$$L_x = Aa \quad (3)$$

$$L_y = Ab \quad (4)$$

where for $N=5$:

$$A = \begin{pmatrix} 1 & X_0 & Y_0 \\ 1 & X_1 & Y_1 \\ 1 & X_2 & Y_2 \\ 1 & X_3 & Y_3 \\ 1 & X_4 & Y_4 \end{pmatrix} \quad (5)$$

$$a = (a_0 \quad a_1 \quad a_2)^T \quad (6)$$

$$b = (b_0 \quad b_1 \quad b_2)^T \quad (7)$$

$$L_x = (x_0 \quad x_1 \quad x_2 \quad x_3 \quad x_4)^T \quad (8)$$

$$L_y = (y_0 \quad y_1 \quad y_2 \quad y_3 \quad y_4)^T \quad (9)$$

Solving equations (3) and (4) for the unknown coefficients a and b takes the form:

$$a = (A^T A)^{-1} A^T L_x \quad (10)$$

$$b = (A^T A)^{-1} A^T L_y \quad (11)$$

The matrix equations (10) and (11) have a solution when the following condition is fulfilled:

$$(A^T A)^{-1} (A^T A) = (A^T A) (A^T A)^{-1} = I \quad (12)$$

where I denotes identity matrix.

B. Obtaining GCP coordinates

As it is illustrated in expressions (3...11), to determine the correction coefficients it is required to know the pixel coordinates of distinctive points $P\{X_i, Y_i\}$ and their corresponding ground coordinates $L\{x_i, y_i\}$. In the direct georeferencing case for the $P\{X_i, Y_i\}$, can be selected the center of the image matrix and the four end corner points. The question here is how to determine the coordinates of the corresponding GCPs $L\{x_i, y_i\}$ when the image is captured by an on-board camera of a UAV.

In order to do this, additional data from the drone's GPS and IMU is required - GPS coordinates and 3-axes inclination. These data are used to associate the $P\{X_i, Y_i\}$ points of the captured image with the actual GPS coordinates of the terrain - Fig.1.

For the final association of the captured image with the real area, it is necessary to know the values of the geographical coordinates of the boundary positions $\{L_0, L_1, L_2, L_3, L_4\}$. To determine the coordinates of the boundary positions, also called control points, it is convenient to apply the methods presented in detail in the material [1].

The inertial coordinate system is denoted as Earth by x axe, North by y axe, and Up by z axe (ENU), it coincides with the reference system. The UAV is in a local coordinate system, named North by x axe, East by y axe and Down by z axe (NED) in the Fig. 1. The coordinates of the UAV concerning the ENU are named the point B (x, y, z). The spatial state of the UAV is set by the angles of the local relative to the inertial coordinate system and for this the yaw, ψ , pitch, θ , and roll, ϕ angles are denoted.

Assumptions: the video camera is fixed at the center of mass of the UAV, the optical axis of the video camera is directed in the positive z direction of the local coordinate system, and the distance D from the Earth's surface are determined with a UAVs flight height via onboard barometric sensor.

The mathematical task consists in determining coordinates $L(x, y, z)$, with input data $B(x, y, z)$, ψ , θ , ϕ , and D . This data is presented by the onboard IMU and GPS.

The mathematical expression, without taking into account the distortions caused by the camera's optical system, has the form:

$$L = R_z(\psi).R_y(\theta).R_x(\phi).N.T_B(x, y, z).T_D \quad (13)$$

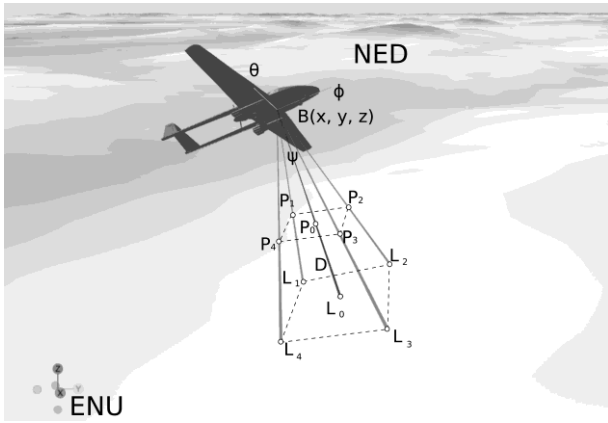


Fig. 1. Association of the captured image with real coordinates

where:

R_z, R_y, R_x – rotation matrices in NED;

N – transformation matrix NED to ENU;

T_B – matrix - UAV position in ENU;

T_D – matrix - distance to L .

For the central point L_0 the determination of the ground coordinates has the form:

$$L_{0,x} = -((D + z) \cos(\varphi) \sin(\theta) + x \sin(\theta) \sin(\varphi) + y \cos(\theta)) \cos(\psi) + (x \cos(\varphi) - (D + z) \sin(\varphi)) \sin(\psi) \quad (14)$$

$$L_{0,y} = -(x \cos(\varphi) - (D + z) \sin(\varphi)) \cos(\psi) - ((D + z) \cos(\varphi) \sin(\theta) + x \sin(\theta) \sin(\varphi) + y \cos(\theta)) \sin(\psi) \quad (15)$$

$$L_{0,z} = -(D + z) \cos(\theta) \cos(\varphi) - x \cos(\theta) \sin(\varphi) + y \sin(\theta) \quad (16)$$

In the proposed mathematical apparatus, the expressions (14) and (15) determine the geographical coordinates of the central position, in Fig. 1 is shown as L_0 . The geographical coordinates of the bounding positions $\{L_1, L_2, L_3, L_4\}$ can be determined by correcting the corresponding values of the angles ψ, θ and the distance D with the values of the horizontal HFoV and vertical VFoV viewing angle of the video camera used. Computational results are applicable when applied in the role of GCP from the earth's surface, which coincide with the limiting end pixels from the sensor matrix of the video camera used.

C. Experimental environment

A quadcopter-type drone was constructed for conducting field experiments. Widespread components were used, such as an F450 frame type, 2212 920KV BLDC motors, and a 4S battery configuration with a capacity of 3300mAh. The flight time is approximately 7 minutes. The main electronic components are a Pixhawk v. 2.4.8 Flight Controller (FC), an M10 GPS module with a QMC5883 electronic compass, a Raspberry Pi 4 Companion Computer (CC), and a video camera with an IMX219-77 optical sensor. The important data regarding the optical sensor for the experiment are: FoV 75° ; Focal

length 2.9 mm; Sensor width 3.67 mm; Sensor Height 2.76 mm; Resolution: width 1920 pixels, height 1080 pixels.

The CC communicates with the FC via a UART port using the MAVLINK2 protocol and monitors the GPIO for a signal to trigger image capture. A software environment has been created with core components and a Python programming tool that includes the pymavlink and picamera2 modules, as well as the EXIFTool image metadata editing tool.

The test flight follows a programmed route with automatic image capture; the route was programmed using the QGroundControl software (Fig. 2). A single image is captured upon sending the MAV_CMD_DO_DIGICAM_CONTROL command via the MAVLINK2 protocol.

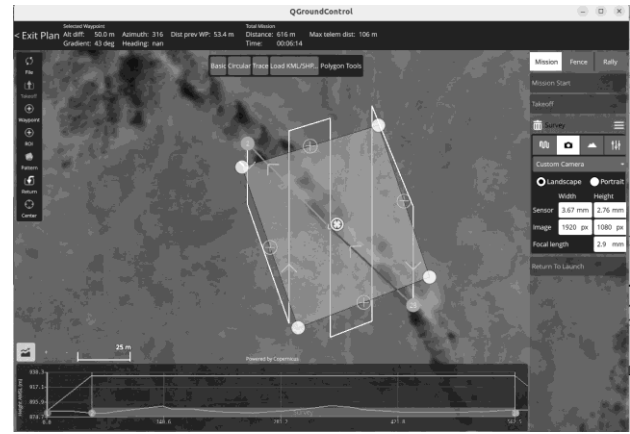


Fig. 2. Flight Plan for Automated Imaging

Upon receiving a capture signal, the CC receives the image in .jpeg format, adds EXIF data regarding the UAV's position and altitude from the FC, and saves the image to the onboard SD card. After the UAV lands, the captured images are transferred to a personal computer (PC).

A software module has been developed to verify the intermediate results of the mathematical processing of the dependencies (10, 11, 14, 15) and to visualize the graphical output of the direct georeferencing of the image. The program code is written in Python 3 and uses the numpy software module. The software module has a simplified graphical interface and functions as a plugin for the specialized product Quantum GIS. As a result of the mathematical processing, a .wld file is automatically generated with the determined values of the coefficients a and b , which QuantumGIS uses to position the image within the screen area.

IV. RESULTS

Table 1 shows the numerical values of the input data used for the mathematical processing required for automated georeferencing. These values are extracted from the EXIF data of the image to be processed. The geographic coordinates from the GPS in the WGS 84 Coordinate

Reference System (CRS) are measured in decimal degrees. For the purposes of the mathematical processing, they have been converted to the CRS UTM zone 34N, where the measurement is in meters.

TABLE 1. INPUT DATA

UAV coordinates B(x, y, z), D	Longitude x		Latitude y		Height	
	WGS 84	23.405555 ⁰	WGS 84	42.571909 ⁰	z	D
	UTM 34N	4716082.54 m	UTM 34N	697433.49 m	897.97 m	50m
Inclination angles ψ (yaw), θ (pitch), ϕ (roll)	ψ		θ		ϕ	
	92.66 ⁰		1.43 ⁰		2.25 ⁰	

The ground control points GCP {L0 ... L4} were located using equations (14) and (15). The coordinate values of these points, which serve as intermediate results in the calculations, are shown in Table 2.

If all the necessary data are available and the dependencies (10, 11) are applied, the desired values for the coefficients a and b are obtained. These values are shown in Table 3. The program-generated .wld file, whose contents are shown in Table 3, allows the automatically georeferenced image to be positioned on the QuantumGIS screen at its actual geographic location in the CRS UTM zone 34N.

To assess the accuracy of the direct georeferencing procedure, the processed image is overlaid as a raster layer on an existing vector map. A fragment of the vector map (part of the road network) obtained from the OpenStreetMap system is shown in Fig. 3. This section of the road network can also be seen in Fig. 2.

V. DISCUSSION

The results of the field experiments provide guidance for improving the tested procedure for direct georeferencing of UAS images. In some cases, a problem was identified with the content of the position and angular deviation data received in the CC from the FC, even though there was no indication of a failed connection between the data ports.

TABLE 2. PRELIMINARY RESULTS

	L ₀	L ₁	L ₂	L ₃	L ₄
x	4716080.64	4716109.39	4716049.92	4716052.01	4716111.48
y	697432.16	697455.93	697453.21	697408.47	697411.18

TABLE 3. CALCULATED COEFFICIENTS

a ₁	-0.0014141557408927606
b ₁	-0.030975223754473605
a ₂	-0.04142991173263196
b ₂	0.0019320338591064577
a ₀	697455.9229481166

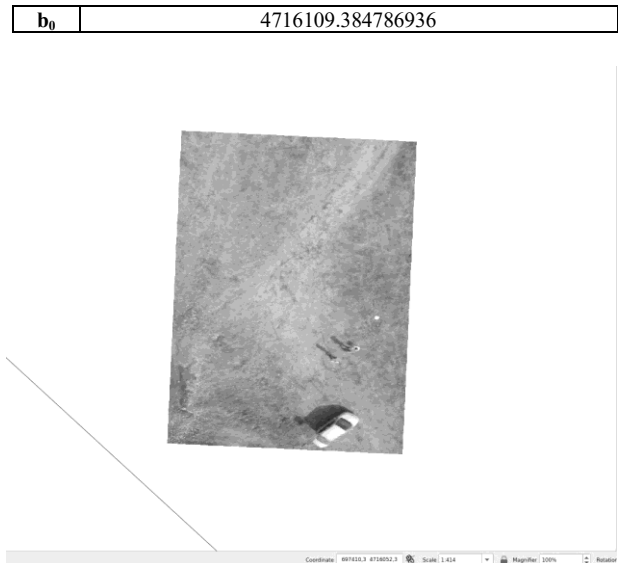


Fig. 3. Result of direct georeferencing

It is necessary for this communication channel to be automatically tested and for a way to be found to include it in the mandatory pre-flight check of the drone.

The goal of aerial photography is to capture images with the highest possible resolution. The maximum resolution of the IMX 219 camera used is 3280 x 2464 pixels. At this resolution, saving a single image to the onboard SD card takes about 5 seconds, which is not acceptable when executing the flight plan. Experiments were conducted with various software modules for controlling the video camera, libcamera and picamera2. We consider the use of picamera2 at a resolution of 1920x1080 pixels with a capture time of 1.5 s to be an acceptable temporary solution.

The Raspberry Pi 4 based CC unit runs on the multi-tasking Bullseye operating system. This could potentially cause a time desynchronization between the image and the data required for automatic georeferencing. Such desynchronization, in addition to the observed delay in capturing a single image, could completely compromise the procedure. It is necessary to explore other hardware solutions for the CC or switch to bare-metal programming on the Raspberry Pi.

Assessing errors in the direct georeferencing process is a crucial step in addressing specific operational and tactical tasks. It is necessary to conduct an in-depth study of the factors that can lead to inaccuracy. Such factors, in addition to the aforementioned possibility of desynchronization of the image, include insufficient precision of GPS coordinates and the determination of elevation using a barometric sensor. Another group of errors is expected to arise from the determination of the angular values used in formulas (14, 15). The impact of angular errors could be reduced by using the Extended Kalman Filter (EKF).

VI. CONCLUSION

This article discusses an approach to the direct georeferencing of aerial photographs, suitable for fully computer-based processing. The mathematical foundations of the georeferencing process are presented, as well as the relationships for determining control points on the Earth's surface. The proposed mathematical framework forms the basis of the program code developed by the authors.

Field experiments were conducted using a quadcopter drone specifically designed for this purpose. A full cycle of software processing was performed on the image data obtained during the experiments. This demonstrated the functionality of the mathematical framework and its readiness for practical application. Potential implementation issues were presented in a discussion format. Guidelines for improving the direct georeferencing procedure were considered.

The results achieved so far provide confidence to proceed with further research into the potential scientific applications of this topic. Research should continue in the following directions: adding a communication channel for real-time processing, testing higher-performance hardware, and transitioning to direct georeferencing of video streams. It is necessary to develop a methodology for determining the accuracy of the automated procedure. As a final result, the authors envision the creation of an original, proprietary hardware and software solution that would serve as a cost-effective replacement for existing commercial RTK systems and find application in military operations.

ACKNOWLEDGEMENTS

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

- [1] A. Kolev, *Command and Control in a Close Geographical Environment*. Sofia: Bulgarian Defense Institute "Professor Tsvetan Lazarov", 2023, ISBN: 978-619-90024-4-5.
- [2] A. J. Ganchev, „Assessment of the reconnaissance capabilities of unmanned aerial vehicles,“ In Proc. International Scientific Conference „Hemus“, 2020, Plovdiv, ISSN 1312-2916, in Bulgarian language.
- [3] A. J. Ganchev, „Role of unmanned aircraft systems for logistics provision and support of military operations to the present moment and in the perspective,“ In Proc. International Scientific Conference „Hemus“, 2022, pp. II-221-231, Plovdiv, ISSN 1312-2916, in Bulgarian language.
- [4] X. Zhuo, T. Koch, F. Kurz, F. Fraundorfer, and P. Reinartz, “Automatic UAV Image Geo-Registration by Matching UAV Images to Georeferenced Image Data,” *Remote Sensing*, vol. 9(4), 376, 2017. [Online]. Available: <https://doi.org/10.3390/rs9040376> [Accessed: Apr. 19, 2026].
- [5] C. A. M. Correia, F. A. A. Andrade, Agnar Sivertsen, Ihannah Pinto Guedes, Milena Faria Pinto, Aline Gesualdi Manhães, and Diego Barreto Haddad, „Comprehensive Direct Georeferencing of Aerial Images for Unmanned Aerial Systems Applications,“ Jan. 13, 2022. [Online]. Available: <https://doi.org/10.3390/s22020604> [Accessed: Apr. 19, 2026].
- [6] D. Liu at all, „Ground Control Point Automatic Extraction for Spaceborne Georeferencing Based on FPGA,“ In Proc. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 2020, pp. 3350-3366, [Online]. Available: <https://doi.org/10.1109/JSTARS.2020.2998838> [Accessed: Apr. 19, 2026].
- [7] D. Liu at all, “On-Board Georeferencing Using FPGA-Based Optimized Second-Order Polynomial Equation,” *Remote Sensing*, vol. 11(2), 124, 10 January 2019, [Online]. Available: <https://doi.org/10.3390/rs11020124> [Accessed: Apr. 19, 2026].
- [8] L. Hill, *Georeferencing: The Geographic Associations of Information (Digital Libraries And Electronic Publishing Series)*. Mit Pr., 2006, ISBN-13:978-0262083546.
- [9] J. Shan, and C. K. Toth, *Topographic Laser Ranging and Scanning: Principles and Processing, Second Edition*. CRC Press, 2018, ISBN 9781498772273.

Multimodal Approach to Teaching English as a Factor in Improving Engineering Students' Research Skills

Nataliia Saienko

*Department of Foreign Languages
Kharkiv National Automobile and Highway University
Kharkiv, Ukraine
saienkonv@ukr.net*

Zhanna Bogdan

*Department of Psychology and Sociology
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
zhanna.bogdan@hneu.net*

Stanislav Larionov

*Department of Psychology and Pedagogy
National Academy of National Guard of Ukraine
Kharkiv, Ukraine
larionov1985@gmail.com*

Tetiana Solodovnyk

*Department of Pedagogy and Psychology of Social Systems Management by the academician I. Zyazyun
National Technical University "Kharkiv Polytechnic Institute"
Kharkiv, Ukraine
tetiana.solodovnyk@khp.edu.ua*

Olena Romanovska

*Department of Psychology, Pedagogy and Professional Communication
O. M. Beketov National University of Urban Economy
Kharkiv, Ukraine
elena_mail2004@ukr.net*

Abstract—In the context of the internationalisation of higher education and the growing role of English as a global language of science and technology, the development of both communicative and research skills among engineering students has become increasingly important. This study investigates the effectiveness of a multimodal approach to teaching English as a factor in improving engineering students' research skills. A quasi-experimental design was employed involving 90 undergraduate students of automotive engineering at Kharkiv National Automobile and Highway University (Ukraine). The experimental group participated in a multimodal English course integrating audiovisual translation, digital learning resources, English for Specific Purposes, and extracurricular research activities, while the control group received traditional language instruction. The effectiveness of the intervention was evaluated using three indicators: information search and analysis skills, English communicative competence, and research self-efficacy. Statistical analysis using Pearson's chi-square test demonstrated significant improvements in the experimental group compared to the control group. The results indicate that the multimodal approach significantly enhances students' information literacy, communicative competence, and confidence in conducting research. The findings highlight the potential of multimodal language instruction to support the development of academic and research competencies among engineering students.

Keywords – *engineering students, foreign language teaching, multimodal approach, research skills.*

INTRODUCTION

In recent decades, researchers aiming to share their findings with the global scientific community have increasingly written and published their articles in English. English has emerged as the lingua franca, providing access to research conducted by scientists worldwide. One indication of English's dominance in the fields of science and technology is that over 90% of indexed scientific articles in the natural sciences have been published in this language [1].

The role of English is increasingly significant due to the internationalisation of higher education. There has been a notable rise in cross-border migration by international students pursuing studies at educational institutions outside their home countries [2]. Host universities are not only in Anglophone countries with native English-speaking populations, but also in many other countries, such as Austria, Denmark, the Netherlands, Greece, Italy, and Spain, that offer their training programs in English [3].

Besides knowledge of so-called General English, which is necessary for survival in the host country, all students entering higher education institutions need to have skills in using academic English to be able to study a variety of subjects, and English for Specific Purposes (ESP) to understand and produce oral and written texts

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.19>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

typical of the specialised subject area they are going to master.

Thus, the relevance of studying English in all its diversity is beyond doubt. Traditionally, students in a foreign language (FL) course master four skills: listening, reading, speaking and writing, mainly based on textbooks created by such respectable publishers as Oxford University Press, Cambridge University Press, Pearson Macmillan Learning, Routledge Taylor & Francis Group, Wiley Publishers, etc. However, modern students live in a world filled with images and sounds mixed with texts, a multimodal world to which they need to adapt and which makes its own adjustments to the approaches to learning a FL.

Multimodality involves using two or more modes of communication to convey the text in the broad sense of this meaning. There are five modes that people use when communicating: 1) linguistic, which focuses on the use of written or spoken language; 2) visual, which prioritises visual images such as symbols, signs, visual design, colour, font type and size; 3) auditory, which focuses on voice, music, sound effects, background noise; 4) gestural, which is realised through facial expressions, hand gestures and body language; and 5) spatial, which involves the physical arrangement of objects.

In modern multimedia resources, communication is realised through images, spoken language, music, and often written texts in the form of subtitles. Such multimodality requires a rethinking of existing approaches to teaching communication, allowing students to read multimodal texts (viewing) and to generate and transmit them (representing) independently. This new type of literacy is vital for the current generation, as it aligns with their way of life and the peculiarities of their interactions with others [4].

Teaching FL, unlike any other activity, requires the broadest range of didactic methods and multimedia tools, as modern research shows [5]. Learning a language with the help of digital technologies can be no less effective than face-to-face training if it is based on a proven, reliable language-teaching methodology that takes into account modern advances in research on the mechanisms of language acquisition and provides a systematic approach to designing the learning process in the context of digitalisation.

The globalised world in which we live, as well as growing academic and scientific mobility, have led to multilingual societies in which linguistic exchanges between native and non-native speakers have become a common practice and reinforce the importance of not only linguistic but also pragmatic competence, which means the ability to convey and perceive the intended message with all its nuances in any socio-cultural context [6]. Modern technologies allow students to go beyond using language only in the classroom and immerse them in real-life out-of-class contexts where they can develop their pragmatic skills in using a FL across a wide range of situations.

Since much modern communication occurs digitally, technology-mediated assignments allow students to engage in socio-pragmatic practice on virtual communication platforms such as email, chat or instant messaging, online forums, and social media. Scholars call this cyberpragmatics, which evaluates situations in terms of what works best or how it can be improved [7].

Currently, linguodidactics is witnessing the increasing popularity of audiovisual translation (AVT) as a new approach to teaching languages and cultures, defined as the transmission of verbal language through audiovisual means and also termed screen, multimedia, or multimodal translation.

Today, audiovisual materials are a key resource in language teaching, providing learners with linguistically and culturally rich, digitally enhanced content that is close to the real world [8].

Khazdouzian et al. [9] studied the impact of audiovisual material on pragmatic language learning and the formation of pragmalinguistic competence, revealing their positive effect. However, as the authors note, although ATV is relevant to FL teaching, only a few studies have explored the relationship between audiovisual resources and pragmatics in language use.

Traditional approaches to teaching FL, which are aimed at increasing students' language proficiency level close to that of native speakers, are losing their relevance, as they no longer prepare students for communication in a world where a third of the planet's population are representatives of different countries and cultures [10].

Students are now expected to be prepared for intercultural communication, which implies that they must be both pragmatically and interculturally competent. Based on this idea, approaches are being developed to ensure students' metapragmatic awareness and strategies for dealing with the hybrid nature of English, its different varieties and the wide range of cultures associated with it [11].

Sal y Rosas Flores [12] highlights the vital importance of encouraging the practical application of research knowledge. This approach not only improves academic performance at the university but also fosters teamwork skills, strengthens interpersonal relationships, and enhances mutual support.

Salazar Peralta et al. [13] emphasise that enhancing research competencies requires the targeted development of students' curiosity and willingness to embrace new ideas, as these qualities form the foundation of their intellectual growth.

Thus, the challenge for technical universities is to find effective ways to combine traditional and digital multimodal methods to prepare prospective engineering professionals for future activities in an English-speaking multicultural environment.

The aim of this study was: 1) to demonstrate the importance of a multimodal approach in enhancing the English language communicative competence of engineering students along with their research skills; and

2) to evaluate the impact of a multimodal English language course, as well as students' participation in extracurricular scientific activities, on their research skills and language proficiency.

To achieve the research aim, the study addresses the following research questions:

RQ1. Does the implementation of a multimodal approach in teaching English improve engineering students' information search and analysis skills compared to traditional instruction?

RQ2. Does participation in a multimodal English course significantly influence students' English communicative competence?

RQ3. Does the multimodal approach combined with participation in extracurricular scientific activities enhance students' research self-efficacy?

RQ4. Are the differences between the experimental and control groups statistically significant according to Pearson's chi-square test?

MATERIALS AND METHODS

Research Design

This study employed a quasi-experimental design involving an experimental and a control group to evaluate the effectiveness of the multimodal approach in teaching English and developing research skills. An experiment was conducted at Kharkiv National Automobile and Highway University (KhNAHU). The following tasks were undertaken during the study: preparing training materials for the experimental work; determining criteria and indicators for assessing students' achievements; forming groups for experimental training; evaluating the initial levels of students' linguistic and research competencies at the pre-experimental stage; conducting the experimental training to test the effectiveness of the approach; assessing the levels of students' linguistic and research competencies at the post-experimental stage; and processing and analysing the experimental data.

Participants

An experimental group (EG) consisting of 46 junior students majoring in automotive engineering was formed to study English using a variety of multimodal methods. In contrast, a control group (CG) of 44 students was instructed using traditional training methods. Both groups attended 90-minute classes once a week during the 2024-2025 academic year.

The study was conducted in accordance with ethical research standards. Participation was voluntary and anonymous. No personally identifiable information was collected, and all data were analysed in an aggregated and anonymised form.

Instructional Intervention

Since motivation is the foundation of any educational activity, one of the primary responsibilities of a foreign language teacher is to create conditions that encourage students to learn the language both in and out of the classroom.

Motivation to learn a foreign language can take various forms: instrumental, expressive, sociocultural, academic [14].

To increase students' interest in language learning and research, we used various examples demonstrating the practical value of language skills for future professional careers. During interviews, students were shown that modern companies prefer specialists who speak several languages, as international projects require effective communication. In engineering, a significant portion of work is conducted in international teams whose members represent different cultures and utilise a variety of digital communication tools, including email, social media, and online video conferencing platforms [15]. Being prepared for this type of interaction directly impacts professional success.

The use of internet technologies in teaching has proven effective in increasing motivation and developing language skills. The internet provides access to a variety of resources: videos, audio recordings, interactive exercises, e-books, articles, and educational platforms. Furthermore, online services allow students to complete assignments and receive quick feedback.

In our experiment, English language instruction was based on a multimodal approach and encompassed three areas: developing general language skills, acquiring English for Specific Purposes (ESP), and developing intercultural competence. The primary teaching method was a communicative approach focused on the practical use of language in real-world situations. Elements of a constructivist approach were also employed, in which students actively build knowledge through personal experience, independent information-seeking, and interaction with the environment.

In the EG, general English instruction was conducted using the Empower textbook [16], available in both print and electronic versions. The educational material was supplemented by original developments by the department's teachers, created using audiovisual technologies.

We adapted audiovisual translation elements using the parallel translation method. Vocabulary was presented simultaneously in written and audio form and posted on YouTube [17]. During deliberate pauses in the recordings, students could repeat language fragments as many times as necessary, which facilitated speech automation and improved pronunciation. In the classroom, the material was reinforced through creative tasks and problem-solving exercises.

This approach is an example of multimodal learning, as it combines several modes of information transmission: linguistic (oral and written speech), visual (images, symbols, design, fonts), and auditory (voice and sound). Additionally, the videos we created were supplemented by internet videos, which introduced two more modes – gestural and spatial.

Such an integrated approach allowed students to independently work with a wide range of materials

covering grammar and cultural content. The video resources covered history, politics, economics, literature, art, cinema, music, and traditions, which contributed to developing readiness for effective intercultural communication.

The ESP competence of automotive engineering students was developed through a course designed in collaboration with instructors in automotive disciplines and made available on the Moodle platform [18] and in traditional paper format [19]. The Moodle course consisted of several thematic modules related to modern automotive engineering, including internal combustion engines, electric and hybrid vehicles, intelligent transport systems, automotive electronics, environmental sustainability, and autonomous driving technologies. Each module integrated multimodal learning resources such as technical texts, glossaries, video lectures, presentations, discussion forums, quizzes, communicative tasks, and self-study assignments. The platform also enabled asynchronous interaction, peer discussion, online assessment, and access to supplementary professional materials, thereby supporting students' independent learning and research activities.

The research skills of prospective professionals were developed both in the classroom and through independent work.

To prepare students for future manufacturing challenges, various methods were employed, including writing an abstract for a research article related to students' future professional activities, preparing an oral presentation on students' coursework in English, examining a professional case study, participating in English-language forums, the simulation of professional situations, business games, and research activities related to the development of new technologies and the forecasting of innovation consequences. Students also engaged in problem-solving scenarios and moral dilemmas, particularly those concerning self-driving cars. For example, should a driverless car sacrifice its passengers to save pedestrians' lives? What should it do if a cyclist suddenly enters its lane – should it swerve into oncoming traffic or collide with the cyclist? Should a robotic car protect its occupants during an accident but endanger a pedestrian crossing the road?

Additionally, the method of presentation, as a specific form of business communication, was widely used in ESP instruction for engineering students. This approach helped students structure their information, persuade potential partners and clients, and develop their rhetorical skills. In preparation for classes, students were required to independently search for relevant information on the course topics, which they then organised into presentations followed by group discussions.

The topics of students' presentations included: "Development of New Fuel Sources for Electrification of Automotive Transport," "Advantages and Disadvantages of Hydrogen Fuel Cells," "Development of Solid-State Batteries," "Fundamental Changes in Business Models of

Automotive Transport," "Improving Charging Infrastructure for Electric Vehicles," "Modern Approaches to Increasing Energy Efficiency in Vehicles," "Next-Generation Batteries," "Solutions to Autonomous Driving Challenges," and "Predictions for the Automotive Industry in Ten Years" and others.

The features of the students' reports and presentations included the productive nature of their speech, independence in selecting content and linguistic means, and a logical structure.

Training materials for developing intercultural competence included the specially designed textbook "Theory and Practice of Cross-Cultural Communication" [20], offered to students in both printed and electronic formats.

A modern textbook is a classic example of a multimodal text, combining several modes of information transmission: written language, images (illustrations, graphs, tables), page layout, typography, and, in digital formats, audio or video. It is important to teach students to understand how these different modes interact to create a communicative act [21].

The textbook we developed is based on a sociocultural approach that views multimodality as part of social practices and cultural contexts. It emphasises how different modes interact and are used together to enhance the meaning of the message in specific social situations [22].

This textbook, drawing on the authors' accumulated theoretical material and practical experience, aims to provide a generalised understanding of a model for teaching intercultural communication in English that future professionals can use to establish intercultural contacts.

The textbook consists of theoretical and practical parts. The theoretical part introduces students to the specific features of intercultural communication, while the second part familiarises them with the characteristics of cultures typical of different regions of the world.

The course material covers a wide range of topics typical of intercultural communication, including types of communication, examples of intercultural differences, ways to improve intercultural communication, specifics of business negotiations, conflict resolution in a multicultural environment, and the concept of ethnicity in the context of intercultural relations. The textbook contains numerous tasks of a reproductive, discussion, and creative nature. Its second part is devoted to comparing the cultures of different countries, solving problematic situations, and completing a case study.

The authors aimed to ensure that the diverse content of the course and the proposed activities would significantly contribute to students' development of intercultural competence and their readiness to connect with representatives of other cultures.

For example, when working with the topic "A guide to international business negotiations", students are offered different tasks at various levels and problematic issues, for

example, a question for consideration: Your company is going to conclude its first export contract. What could be done to secure this contract and establish long-term relationships with your prospective partners?

In the second part of the textbook for comparing different cultures, the following tasks can be solved:

a) Write a portrait of a typical/average Englishman, Australian, Spaniard, Arab, etc. Then comment on their similar features and cultural differences.

b) Write a list of DOs and DON'Ts for a friend of yours who is going as a tourist to China, the United Arab Emirates, etc.

In addition to the text material, each topic of the textbook was accompanied by a video of either a general cultural nature (for example, countries and continents, 7 wonders of the world, the best museums in the world, etc.), or touching on aspects of intercultural interaction relevant to the topic), for which tasks were developed to understand the content of the video and discuss it.

Besides, the Department of Foreign Languages organised regular competitions for student research papers in foreign languages on various topical cultural and socio-humanitarian themes. Some of the themes included: "What Inventions Await Us in the Future?", "Global Challenges of the 21st Century," "Multicultural Communities: How Do They Coexist?", "Volunteering as a Socio-Cultural Phenomenon in Modern Society," "Modern Education: The Biggest Threats and Challenges," and "What Are the Potential Benefits and Dangers of Artificial Intelligence?"

At KhNAHU, like in many other higher education institutions, there is a tradition of holding annual student scientific conferences. In the experimental year, the topics covered numerous technical, economic, cross-cultural and social aspects, showcasing a wide range of student interests in automotive engineering as well as humanitarian problems. Among others, they focused on the prospects of using artificial intelligence in the automotive industry, environmental issues related to transportation, and the challenges of post-war restoration of Ukraine's transport industry.

In preparation for their presentations, students needed to study substantial material on their chosen subjects, master multimedia presentation techniques, develop rhetorical skills, and learn to conduct debates.

RESULTS AND DISCUSSION

The following criteria were established to assess students' communication skills and their abilities in research activities: 1) the cultivation of information search and analysis skills; 2) the development of English communication competencies; and 3) the enhancement of research self-efficacy.

Development of Information Search and Analysis Skills

The first research question concerned the development of students' information search and analysis skills. These skills were evaluated based on the ability to locate,

evaluate, and use scientific information obtained from digital sources.

Information search and analysis skills are an important element of a professional competence in the information society, as they help actively leverage the capabilities of computer networks to facilitate a fruitful exchange of information. We believe that a prospective engineering professional should know the methods of information search and analysis, be able to find, differentiate and process information, use modern means of communication, and receive and exchange information about the development of their field through personal contacts, membership in a particular scientific community, work on the internet, participation in real and web conferences, etc.

Information search and analysis skills may be considered sufficiently developed if students master the methods and culture of working with information obtained on the internet, show interest in search activities, and strive to analyse scientific and reference sources. The skills are not sufficiently developed if students are indifferent to seeking new information; they lack the skills to work with scientific and reference sources and modern communication tools.

We used the ACRL framework [23] aligned with the purpose of our study to assess the ratio of students in the EG and CG participating in research activities, including student competitions, conferences, roundtable discussions, and publications in scientific journals.

An analysis of the dynamics of information search and analysis skills revealed a significant positive trend in the EG compared to the CG (see Table I).

TABLE I TRENDS IN THE DEVELOPMENT OF INFORMATION SEARCH AND ANALYSIS SKILLS

Criteria and indicators	EG (n = 46)		CG (n = 44)	
	Pre-test	Post-test	Pre-test	Post-test
1	2	3	4	5
Information search and analysis skills:				
Developed information search and analysis skills	31.3	82.4	32.1	59.4
Insufficient motivation and poor information skills	68.7	17.6	67.9	40.6

Note. Values represent percentages of respondents. EG = experimental group; CG = control group.

Pearson's χ^2 test revealed statistically significant differences in the development of information search and analysis skills among students in the EG before and after the formative stage of the experiment ($\chi^2 = 22.44$; $p <$

0.001). Changes were also recorded in the CG, but they were less pronounced ($\chi^2 = 5.55$; $p < 0.05$). These data confirm the effectiveness of the developed teaching method.

Development of English Communicative Competence

The second research question examined the effect of the multimodal course on students' English communicative competence.

To assess communicative competence, a language test was developed, including tasks in general English and ESP. The test consisted of 100 items of various types: multiple-choice, matching, true/false, fill-in-the-blank, and listening, speaking, and creative writing. The assessment was based on quantitative indicators using Bepalko's methodology [24], which involves determining the levels of material acquisition: recognition, reconstruction, productivity, and creativity. This approach allows for an objective assessment of the degree of comprehension and memorisation of the material, its level of complexity, and the degree of automation of acquired skills.

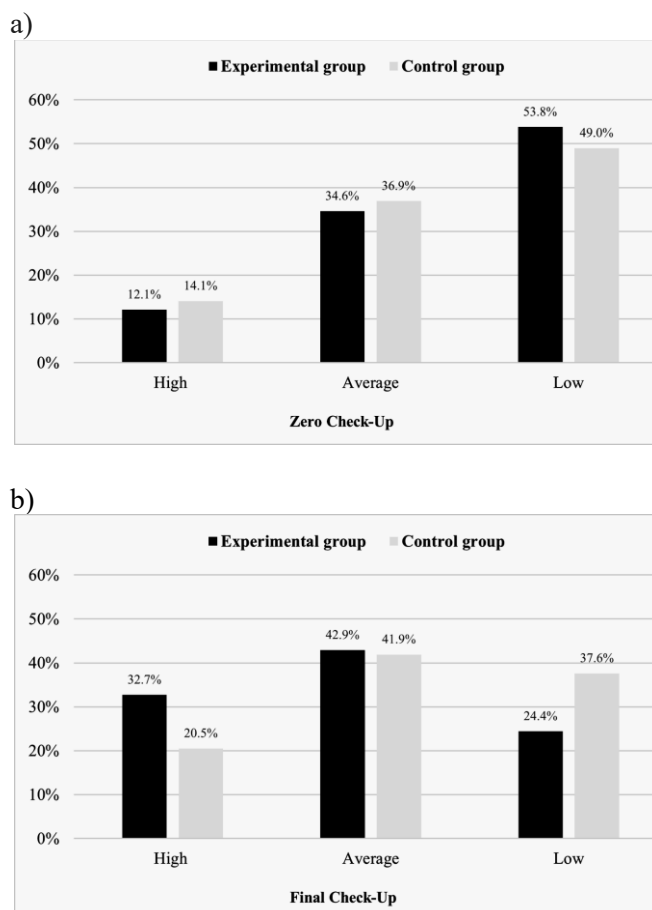


Fig. 1. Trends in the Development of English Communication Competence Levels (%)

After completing the test, the number of correct answers was counted to determine the student's language proficiency level. A score of over 80% was considered high, 60% to 80% – intermediate, and less than 60% – low. The distribution of students by English proficiency level is shown in Fig. 1.

Statistical analysis confirmed the significance of these changes. Pearson's chi-square test showed statistically significant differences between the pre-test and post-test results in the EG ($\chi^2 = 8.4$, $p < 0.05$). In contrast, the changes observed in the CG did not reach statistical significance ($p > 0.05$).

These results suggest that the integration of multimodal learning resources, audiovisual materials, and communicative tasks contributed to a measurable improvement in students' English communicative competence.

Development of Research Self-Efficacy

The third research question focused on the development of students' research self-efficacy, defined as students' confidence in their ability to perform key stages of the research process.

To assess research self-efficacy, an adapted version of the Research Self-Efficacy Scale, initially developed by Holden et al. [25], was used. This instrument measures students' confidence in completing the main stages of research: problem formulation, literature review, methodology selection, data processing, and writing a scientific paper.

The scale was adapted to meet the objectives of the current study with an emphasis on key components of students' research competence. The wording of all items was revised to reflect Bandura's self-efficacy theory. Ratings were conducted on a five-point Likert scale, ranging from 1 ("not at all confident") to 5 ("very confident") (see Table II).

The construct validity of the instrument is supported by the theoretical consistency of all items, which are designed to measure a single latent construct – research self-efficacy. The scale's unidimensional structure is consistent with previous research in this area.

At the end of the experimental year, after gaining experience through research activities, students completed a self-assessment scale. A comparative analysis of the results of the experimental and control groups revealed apparent quantitative differences in the level of development of research competencies. According to descriptive statistics, the average score in the EG was 4.44 on a five-point scale, while in the CG it was 2.78. This difference of 1.66 points indicates a higher level of skill development among students in the EG.

The EG demonstrated consistent positive dynamics in virtually all research skills. The most significant differences ($\Delta M = 2-3$ points) were observed in higher-level skills: interpreting results, formulating conclusions based on data, justifying methodology, and written and

oral scientific communication. This indicates the development of complex analytical and reflective skills.

Moderate differences ($\Delta M = 1-2$ points) were found in procedural skills: formulating research problems, selecting methods, planning the study, and conducting quantitative and qualitative data analysis. The stability of these differences across several indicators suggests a systemic training effect.

TABLE II ADAPTED RESEARCH SELF-EFFICACY SCALE

Item No.	Item statement	Scale
1.	I am confident in my ability to formulate a relevant scientific research problem.	1-5
2.	I am confident in my ability to clearly define the purpose and objectives of the research.	1-5
3.	I am confident in my ability to find relevant scientific sources on the research topic.	1-5
4.	I am confident in my ability to critically evaluate scientific literature.	1-5
5.	I am confident in my ability to formulate research questions or hypotheses.	1-5
6.	I am confident in my ability to select appropriate research methods in accordance with the research purpose.	1-5
7.	I am confident in my ability to develop a coherent research design.	1-5
8.	I am confident in my ability to justify the choice of research methodology.	1-5
9.	I am confident in my ability to collect empirical data in an appropriate manner.	1-5
10.	I am confident in my ability to use quantitative data analysis methods.	1-5
11.	I am confident in my ability to use qualitative data analysis methods.	1-5
12.	I am confident in my ability to interpret obtained research results.	1-5
13.	I am confident in my ability to draw justified conclusions based on empirical data.	1-5
14.	I am confident in my ability to discuss research results in a scientific context.	1-5
15.	I am confident in my ability to formulate research results in written form.	1-5
16.	I am confident in my ability to use an appropriate scientific writing style.	1-5
17.	I am confident in my ability to present research results orally (e.g., presentations or reports).	1-5
18.	I am confident in my ability to independently complete a research project.	1-5

The CG demonstrated lower mean scores and less variability, reflecting a predominantly moderate level of research competence.

Thus, the collected data were analysed using descriptive statistics and Pearson's chi-square (χ^2) test to determine whether the observed differences between

groups and experimental stages were statistically significant. A significance level of $p < 0.05$ was adopted to determine statistical significance.

Overall, the EG demonstrated more pronounced and systematic improvements in information search and analysis, language proficiency, and research skills. Differences in the final distribution of results indicate a more substantial developmental effect of the applied method, particularly in increasing motivation to work with sources, confidence in public speaking, and the effective use of research materials.

The study also found that students prefer searching online because it provides quick access to a wide range of resources, including scientific articles and lectures from leading universities. The online environment offers a range of convenient learning formats: reading, watching video lectures, listening to podcasts, or participating in interactive courses. Furthermore, digital resources are updated more quickly than print publications, enabling self-paced learning.

However, searching for information online also has its drawbacks: information overload, issues with source reliability, dependence on technical specifications, intrusive advertising, and privacy risks. Printed publications, on the other hand, offer more structured, curated material, though they lag the internet in terms of update speed and searchability.

Experience in teaching ESP has shown that students are not always sufficiently engaged, despite the course's direct relevance to their future profession. To enhance interest, it is important to connect the learning material with real-world professional tasks. This can be achieved through practical assignments involving information search and analysis, presentation preparation, role-playing, simulated work situations, and gamification elements. The use of professionally oriented articles, videos, and case studies makes learning more meaningful and practical.

Increasing students' confidence in independent research in English requires a comprehensive approach that includes practical assignments, motivational strategies, the use of digital technologies, and the development of communication skills. The use of authentic materials related to the future profession plays an important role, as does the development of self-management skills such as goal setting, time management, and working with information resources.

The audiovisual method used in the study has both advantages and limitations. Its strengths include improved listening and visual comprehension, automated speech skills, and increased learning intensity. However, excessive focus on limited language material can reduce the depth of learning and the development of analytical thinking. Rapid acquisition of speech patterns ensures functional competence, but does not always guarantee full language proficiency. Despite certain limitations, this digital method appears promising and requires further research and improvement.

The textbook "Theory and Practice of Cross-Cultural Communication" demonstrates the effectiveness of sociocultural and multimodal approaches to developing intercultural communicative competence. Of particular value is the assignments' focus on simulating real-life professional situations (e.g., international negotiations), which enhances the practical nature of the training. At the same time, a discussion of the results calls for further empirical confirmation of the long-term impact of multimodal resources on the sustainability of acquired intercultural skills and their transfer to real-world professional contexts.

CONCLUSIONS

Key components of professional competence for future engineers include developed communication skills, intercultural competence, the ability to work effectively in international teams, and proficiency in English as a professional language.

Technical universities play an important role in preparing specialists for scientific and technical work in a globalised world. This training requires special attention to the study of foreign languages and the development of research competencies that ensure graduates' international competitiveness.

Modern communication is multimodal and encompasses linguistic, visual, auditory, gestural, and spatial modes of information transfer. This is evident in the widespread use of videos, blogs, presentations, web resources, and other digital formats. Therefore, students must be prepared not only to perceive but also to produce multimodal texts in accordance with the demands of the modern professional environment.

The digital space offers extensive access to English-language professional development resources. These resources foster students' cognitive and research interests and can be used in formal education, through independent work and informal learning. Informal learning includes participation in scientific competitions, conferences, and roundtables, as well as the preparation of publications.

To effectively develop future engineers' communicative competence and research skills, it is necessary to design and implement innovative multimodal courses. Such courses develop modern academic and digital literacy and prepare students for professional work in the dynamically evolving digital space.

REFERENCES

- [1] R. E. Hamel, "El campo de las ciencias y la educación superior entre el monopolio del inglés y el plurilingüismo: Elementos para una política del lenguaje en América Latina," *Trab. Linguist. Apl.*, vol. 52, pp. 321–384, 2013. <https://doi.org/10.1590/S0103-18132013000200008>
- [2] A. Perez-Encinas and J. Rodriguez-Pomeda, "Geographies and cultures of international student experiences in higher education," *J. Int. Stud.*, vol. 9, no. 2, pp. 412–433, 2019. <https://doi.org/10.32674/jis.v9i2.271>
- [3] Z. Köylü and N. Tracy-Ventura, "Learning English in today's global world: A comparative study of at home, anglophone, and lingua franca study abroad," *Stud. Second Lang. Acquis.*, vol. 44, pp. 1330–1355, 2022. <https://doi.org/10.1017/S0272263121000917>
- [4] K. Donaghy, S. Karastathi, and N. Peachey, *Multimodality in ELT: Communication Skills for Today's Generation*. Oxford, U.K.: Oxford Univ. Press, 2020.
- [5] S. Zeng, "The potential of online technology for language learning," *English Lang. Teach.*, vol. 13, no. 10, pp. 23–37, 2020. <https://doi.org/10.5539/elt.v13n10p23>
- [6] A. Sánchez-Hernández and J. Barón, "Teaching second language pragmatics in the current era of globalization: An introduction," *Lang. Teach. Res.*, vol. 26, no. 2, pp. 163–170, 2022. <https://doi.org/10.1177/13621688211064931>
- [7] M. González-Lloret, "Technology-mediated tasks for the development of L2 pragmatics," *Lang. Teach. Res.*, vol. 26, no. 2, pp. 173–189, 2022. <https://doi.org/10.1177/13621688211064930>
- [8] N. Talaván, A. Fernández-Costales, and J. Lertola, *Didactic Audiovisual Translation and Foreign Language Education*. New York, NY, USA: Routledge, 2024.
- [9] Y. Khazdouzian, J. Barón, and M. L. Celaya, "When watching is not enough: The effects of captions on L2 pragmatics acquisition and awareness," *RAEL: Rev. Electrón. Lingüíst. Apl.*, vol. 19, pp. 90–107, 2021.
- [10] D. Crystal, "Two thousand million? Updates on the statistics of English," *English Today*, vol. 24, no. 1, pp. 3–6, 2008. <https://doi.org/10.1017/S0266078408000023>
- [11] Z. Tajedin and M. Alemi, Eds., *Pragmatics Pedagogy in English as an International Language*. London, U.K.: Taylor & Francis, 2021, pp. 1–18. <https://doi.org/10.4324/9781003097303-1>
- [12] R. R. Sal Y Rosas Flores, "Factors of learning strategies contributing to students' research skills," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 19s, pp. 825–833, 2025. <https://doi.org/10.52783/jisem.v10i19s.3119>
- [13] J. Salazar Peralta, J. Meléndez Cruz, and M. Cardenas Rivera, "Students' research skills: A systematic review article," *Rev. Invecom*, vol. 6, no. 1, pp. 1–11, 2026. <https://doi.org/10.5281/zenodo.15866881>
- [14] O. Matviyas, "Modern approaches to the methodology of teaching English in higher educational institutions," *Sci. Bull. Vinnytsia Acad. Contin. Educ., Ser. Pedagogy Psychol.*, no. 4, pp. 77–85, 2023. <https://doi.org/10.32782/academ-ped.psyh-2023-4.13>
- [15] A. Kamp, *Engineering Education in a Rapidly Changing World*, 2nd rev. ed. Delft, Netherlands: TU Delft, 2016. <https://doi.org/10.59490/mg.71>
- [16] A. Doff, C. Thaine, H. Puchta, J. Stranks, P. Lewis-Jones, and G. Burton, *Empower B1*. Cambridge, U.K.: Cambridge Univ. Press, 2022.
- [17] *English from 0 to B2: Advanced Lexical Course of English*. [Online]. Available: <https://www.youtube.com/channel/UCF9gPDPSDh0djmvmv8ZyU6A>
- [18] *Foreign Language (Professionally Oriented) for Students of the Automotive Faculty*, 2022. [Online]. Available: <https://dl2022.khadi-kh.com/course/view.php?id=3214>
- [19] N. V. Saienko, *English for Automotive Engineers: A Textbook for Students of Automotive Specialties*. Kharkiv, Ukraine: KhNAHU, 2023. [Online]. Available: <https://dspace.khadi.kharkov.ua/handle/123456789/11215>
- [20] N. V. Saienko and V. Monev, *The Theory and Practice of Cross-Cultural Communication*. Kharkiv, Ukraine: KhNAHU, 2025, in press.
- [21] S. Mavridi and D. Xerri, *English for 21st Century Skills*. Newbury, U.K.: Express Publishing, 2020.
- [22] G. Kress, *Multimodality: A Social Semiotic Approach to Contemporary Communication*. London, U.K.: Routledge, 2010.
- [23] Association of College and Research Libraries, *Framework for Information Literacy for Higher Education*. Chicago, IL, USA: ACRL, 2016.

- [24] E. N. Gerasimov and M. E. Kudryashova, "Update and modernization of key concepts of the theory of pedagogical systems of V. P. Bespalko," *Universum: Psychol. Educ.*, no. 4(5), 2014. [Online]. Available: <http://7universum.com/ru/psy/archive/item/1210>
- [25] G. Holden, K. Barker, T. Meenaghan, and G. Rosenberg, "Research self-efficacy: A new possibility for educational outcomes assessment," *J. Soc. Work Educ.*, vol. 35, no. 3, pp. 463–476, 1999. <https://doi.org/10.1080/10437797.1999.10778982>

Methods for Data Archiving and Recovery Using Artificial Intelligence

Elena Shtereva

Naval Academy "Nikola Y. Vaptsarov"

Varna, Bulgaria

73 Vasil Drumev St.

eshtereva@naval-acad.bg

ORCID: 0009-0008-1799-7106

Abstract - In the face of digital renewal, data is one of the most valuable stockpiles for any organization. They not only facilitate operational activity, but also play an important role in strategic decision-making. This data can include everything from clinical trials and client databases, to reports and internal communications. Through data processing, companies can identify weak links in their operations and offer solutions to improve them.

Incorporating artificial intelligence into data archiving processes represents a big step in information management. Methods using artificial intelligence are automated, intelligently indexed, and offer search, which significantly increases the efficiency and accuracy of archival systems.

The report presents methods that compare the evolution and improvement of data archiving and recovery processes through artificial intelligence, while addressing potential challenges and limitations. An assessment of the risk of data loss in artificial intelligence systems was made using the Weibull model to predict failures. A Bayesian distribution flowchart has been developed, demonstrating the efficiency of a data backup system using implemented AI.

Keywords - Artificial Intelligence (AI), Data Backup and Recovery, Optimization.

I. INTRODUCTION

In a time of accelerated development of information technologies and constantly increasing volumes of data, maintaining their reliable protection and storage becomes a top priority. Data backup plays a key role in ensuring its integrity and the ability to recover information in case of incidents. Therefore, the choice of appropriate methods for data backup is essential for the effective functioning of information systems.

Differential backups accumulate large backups over time because it copies all the changes from the last full backup. Recovery is slow and complicated because it requires a sequential restore from multiple backups.

The same increase in disk space used is also seen with incremental backups, which require multiple small backups and make backups complex. With incremental backups, recovery is faster, but over time, the backups become larger. Damage or loss of intermediate backups makes data recovery incomplete or impossible. Often, there is a lack of reliable verification of the integrity of backups.

Conventional backup methods have been proven over time, but with advances in technology, big data, and fast recovery requirements, they are becoming less and less effective. Traditional methods are difficult to adapt to cloud environments, dynamic infrastructures, and big data. Limited flexibility and scalability make it difficult to quickly restore individual files or versions. This necessitates the introduction of innovative approaches to ensure better optimization, reliability, and flexibility.

AI-assisted data backup changes classic approaches by adding intelligence, automation, and adaptability to backup and backup systems. Backup focuses on important data, which optimizes resources and speeds up the process.

II. APPROACHES TO DATA BACKUP AND RECOVERY USING ARTIFICIAL INTELLIGENCE.

A. Dynamic archive management with integrated AI

Intelligent data classification and prioritization using artificial intelligence analysis data and determines which files or groups of data are critical, frequently used, or strategically important. Machine learning can recognize commonly used and important files that need to be backed up periodically.

The result of using artificial intelligence in data backup is increased efficiency in optimizing resources, automating processes, higher reliability in automatic detection and error correction. Fast data recovery with intelligent selection of versions, priorities and security through early

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.82>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

threat detection with quick responses.[11] Automatic file classification and prioritization uses machine learning, with models such as Random Forest, Support Vector Machine (SVM) or neural networks to analyse the metadata and contents of the files. [16] Critical documents are automatically marked and a more frequent schedule for their backup is set, and for unimportant or old files, archiving is done less frequently. Time series and forecasting models, Long Short-Term Memory (LSTM) or neural networks, analyse system load and data usage to predict when backups will take place without disrupting users. Backups are scheduled at night or during periods of low activity, but dynamically adapt to changes in workload. [5] To protect the archive from anomalies, algorithms, such as Isolation Forest or Autoencoders, are used to detect unusual patterns in the archive files that trigger a recovery process from an older archive. AI analysis file types and content to choose the most efficient method of compression and deduplication. [1] With built-in AI modules - Cohesity and Rubrik, as well as Z standard, LZMA, or Brotli algorithms with machine learning, the system dynamically selects compression with a higher text ratio and faster video speed, which reduces time and space used. When restoring via a chatbot using Natural Language Processing (NLP), models such as GPT or BERT are applied, which allow you to restore the last created archive and automatically start the process. When using a GPT model, it is not necessary to determine the location of the archive in advance. To implement such solutions, tools such as the OpenAI GPT API, Dialogflow, and Microsoft Bot Framework are used.

B. Backup methods and AI data recovery systems

A study of archiving methods using artificial intelligence has been carried out, which allow efficient backup through intelligent compression, storage optimization and improved accuracy in digitization of archives. The results of the study are summarized in Table 1, presenting the potential problems and limitations associated with the implementation of such technologies.

TABLE 1 METHODS OF ARCHIVING USING ARTIFICIAL INTELLIGENCE.

<i>Methods and research</i>	<i>Indicator</i>	<i>Results</i>
Study of data compression with AI	High compression	~90% compression using AI [10],[15]
Perceptron-parallelized data compression	Indicative framework with three-layer perceptrons (machine learning) and parallelization within blocks	Up to 17.78% improvement in speed over SZ2.1 PW REL in experiments [7]
3D and multimedia archives	Collaborative quantization with common codes and conditional	Compresses 3D scenes to the kilobyte range with better compression and adaptability for updates [9]

	decoding from photos	
Model data trimming	Server Merge and Separation of Local Models for Parameter Change and Communication	Achieves very high compression rates (>99.7%) with minimal quality loss (<1.18%) in IoT/FL scenarios [2]
Optimizing Forest Data	Predictive accuracy	$R^2 = 0.9965$ (train), $R^2 = 0.9520$ (test) for cloud storage performance optimization.[14]
Media digitization of an archive	Digitization accuracy	Improved from 92.3% output level to 95.7% after setup. [3]

The statistical indicator R^2 in Table 1 is applied to measure how well a model explains the variation in the observed data.

The AI analyses the version of the files using contextual data and the most appropriate version for recovery. An example of this is documents with multiple revisions, of which the AI suggests the most relevant version according to user demand or criticality. The AI detects abnormal activity in the archives, which is an indication of malware. It automatically triggers a restore from the last healthy backup and prevents data loss. Examples of AI software bundles that detect threats in data backup and recovery are listed in Table 2.

TABLE 2. EXAMPLES OF AI BUNDLES.

<i>Bundle</i>	<i>Applications of artificial intelligence</i>
Rubrik	Automate backup and recovery, analyze risks and priorities with machine learning [12]
Cohesity	Intelligent deduplication and cybersecurity with artificial intelligence [4]
Veeam (с AI модули)	Analytics and automation of backup processes, anomaly detection [13]
IBM Spectrum Protect	Artificial Intelligence for Data Management and Backup Optimization in Hybrid Clouds
Commvault	Manage backups and backups using AI

From the data presented in Tables 1 and 2, the advantages of using artificial intelligence over standard data archiving methods can be summarized:

- The reliability and integrity of archived data is increased by using automatic restoration or the creation of new backups without human intervention.
- Artificial intelligence optimizes deduplication processes by intelligently recognizing duplicate or similar data. Compression adapts according to data type, achieving better results [10].
- Integration of chatbots that, through natural language, allow users to request the restoration of specific files or versions.

C. Monitoring data in systems with integrated AI

When an incident occurs in a backup system, the AI consolidates hundreds of alerts, speeding up analysis by 96%. Behavioral profiling in Extended Detection and Response reduces false alerts by 89%, and automated AI scenarios master ransomware 18 times faster than manual response. As a result, the average time to detect a problem or incident and the average response and recovery time after an incident are reduced from hours to minutes. [17],[20],[22],[23]

AI systems predict when is the best time to backup. A calculation based on Bayes' theorem (1) is applied in combination with time series and anomaly analysis. [18]

The Bays formula has the form (1):

$$P\left(\frac{C}{D}\right) = \frac{P(D/C)*P(C)}{P(D)}, \quad (1)$$

where:

P(C/D) (posterior probability), is the probability that hypothesis C is correct after observing data D (in case of anomalies or risk of loss);

P(D/C) (likelihood), is the probability of occurrence of the observed data D if there are anomalies or risk of loss, in hypothesis C;

P(C) (prior probability) is a preliminary probability of hypothesis C before presenting the data (based on the history of the frequency of failures and the risk of loss);

P(D) (marginal probability) is the total probability for the D data;

All of these quantities are dimensionless and take values between 0 and 1 (or between 0% and 100% if expressed as a percentage).

The risk of data loss is assessed based on usage patterns and potential failures. The initial probability P(C) changes as new information enters the archive system, allowing dynamic management of archives to minimize the impact of system failures.[19],[21] The prediction of failures in it is based on the Weibull distribution model (2), which uses statistics on time to failure to estimate the probability and frequency of future failures. [22]:

$$f(t) = \frac{\beta}{\eta} \left(\frac{t}{\eta}\right)^{\beta-1} e^{-(t/\eta)^\beta}, \quad (2)$$

where:

t is the time to failure

η is scale parameter (average time to failure)

β is shape parameter (determines the shape of failures, accidental failures).

D. Results and discussion of the research done

Using the Weibull model helps administrators predict future hardware failure and save information in time. No time is wasted on too frequent backups of robust systems, and efforts are focused where the statistical model predicts a problem. When a predefined threshold is reached, the system automatically initiates a backup of critical data, migrates it to more reliable media, and takes risky devices out of service. This avoids unnecessary backups of stable systems and concentrates resources on components with the highest probability of failure.

Figure 1 shows a flowchart of an algorithm linking the logic and communication of archiving processes to the use of Weibull's model. The algorithm follows the steps:

1. The administrator configures the backup threshold.
2. The monitoring system sends data to the Weibull model.
3. The Weibull model returns a probability of failure.
4. If the risk is high→ Backup Manager starts a backup.
5. Storage devices receive the command to transfer and decommission.

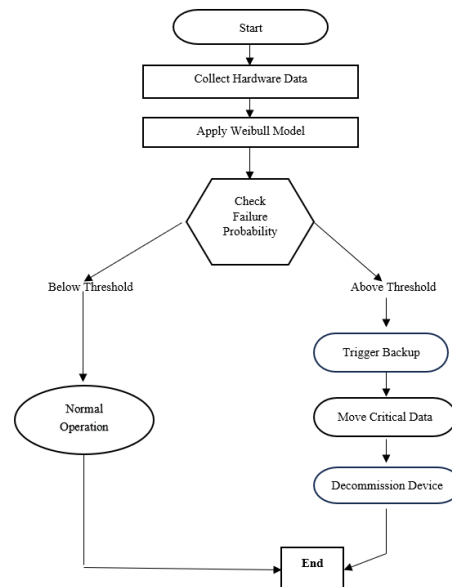


Fig. 1. Flowchart of an archiving algorithm according to the Weibull model

Table 3 presents calculations with a Bases classification of data backup with a traditional method and with AI deployed over a period of 1 year. The efficiency of the backup system can be evaluated through indicators such as backup frequency, resource utilization, recovery time and resistance to data loss. Within a one-year period, there are significant differences between traditional reactive systems and intelligent proactive solutions based on predictive models.

TABLE 3. COMPARISON OF THE PERFORMANCE OF BACKUP SYSTEMS OVER A PERIOD OF 1 YEAR

Indicator	Traditional backup	AI - Based Backup
A priori probability P(C)	0.7	0.3
Probability of correct classification P(D/C)	0.1	0.8
Accuracy of classification P(C/D), conditional probability	0.226	0.774
Paramet η (Weibull)	8 years	10 years
Parameter β	1.5	1.5
System reliability after 1 year R(t)	0.957	0.976
Performance Index E	0.216	0.756

To calculate the reliability of a backup system for 1 year, Weibull's formula was used:

$$R(t) = e^{-(t/\eta)^\beta} \quad (3)$$

where:

t - time of use of the backup system;

β - increasing probability of failure of the backup system;

η - average time to failure of the backup system.

For the calculation of **R(t)** according to formula (3) the parameters are given the following values: **t** = 1 year; average time to failure for traditional systems **η** = 8 years, average time to failure for artificial intelligence systems **η** = 10 years; **β** = 1.5

The calculated value of the reliability of the traditional backup system for 1 year is **R (1)** =0.957, and for an AI system – **R (1)** =0.976. The AI system is 1.9% more reliable than the traditional one.

The calculation of the efficiency index E, which combines the accuracy of the model with the temporal reliability of a backup system, is performed according to formula (4). P(C|D) is a conditional probability reflecting the accuracy of the classification.

$$E = P(C|D) \times R(t) \quad (4)$$

where:

$$P(C_1) = 0.7$$

$$P(C_2) = 0.3$$

$$P(D|C_1) = 0.1$$

$$P(D|C_2) = 0.8$$

$$P(D) = 0.8 \times 0.3 + 0.1 \times 0.7 \rightarrow P(D) = 0.31$$

$$P(C_1|D) = \frac{0.1 \times 0.7}{0.31} \rightarrow P(C_1|D) = 0.226$$

$$P(C_2|D) = \frac{0.8 \times 0.3}{0.31} \rightarrow P(C_2|D) = 0.774$$

For the traditional archiving system, the value of $E=0.226 \times 0.957=0.216$, and for the archiving system with integrated artificial intelligence: $E=0.774 \times 0.976=0.756$. The results obtained show that the archiving system with integrated AI technology is 52% more efficient than the traditional archiving method.

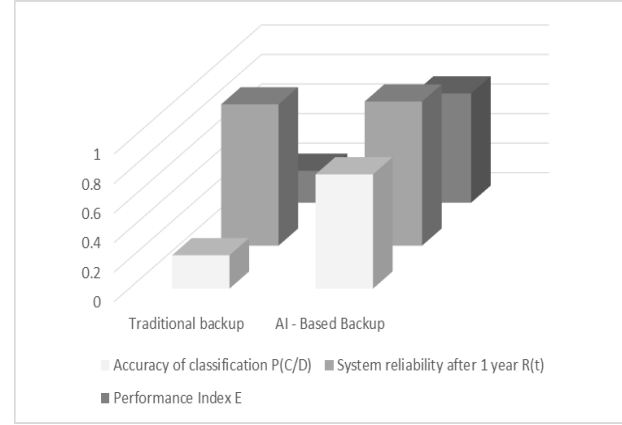


Fig. 2. Result of system research within 1 year

From the diagram in Figure 2, it can be seen that an archiving system with integrated AI is more efficient than a system using archiving with traditional methods. While both systems manage to reliably preserve data after a year of operation, the traditional system has a serious problem with its proper classification. An archiving system with integrated AI solves this problem, providing both high reliability and high accuracy of classification, which logically leads to its high efficiency index.

III. CONCLUSION

Traditional backup methods, although proven over time, turn out to be insufficiently effective in the conditions of dynamic infrastructures, cloud environments and the need for quick access to specific data. Their limited flexibility and scalability require the search and implementation of modern solutions. In this sense, the use of artificial intelligence has established itself as a key factor for the modernization of data archiving processes. The research on predicting failures in archiving systems demonstrates the potential of the proposed approach for improving reliability and supporting data management processes. By assessing the probability of failure, the backup system allows taking preventive actions such as archiving critical information, migrating to more secure media, and decommissioning risky devices. Fault forecasting helps in a more rational use of resources and reduces unnecessary data backup operations. The result is a balance between efficiency and reliability of the infrastructure. Future research in this area can be aimed at studying an archiving system with the integration of machine learning methods to improve the accuracy of Weibull model predictions through real-time analysis. It is also possible to implement adaptive algorithms that dynamically change the threshold values according to the load conditions and the backup period. Monitoring of the backup system with risk visualization will help for automated decision-making through artificial intelligence.

Integration with cloud infrastructure will allow scalable backups, as well as faster recovery in case of incidents.

IV. ACKNOWLEDGMENTS

This report was financed by the Ministry of Education and Science under the National Science Program "Security and Defense", carried out in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and adopted by Decision of the Council of Ministers No. 731 of October 21, 2021. The material reflects only the author's opinion and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] J. S. Caicedo-Vivas and W. Alfonso-Morales, "Short-term load forecasting using an LSTM neural network for a grid operator," *Energies*, vol. 16, no. 23, p. 7878, 2023, doi: 10.3390/en16237878.
- [2] G. Colavizza et al., "Archives and AI: An overview of current debates and future perspectives," *Journal on Computing and Cultural Heritage*, vol. 15, no. 1, pp. 1–15, 2022, doi: 10.1145/3479010.
- [3] A. L. Cushing and G. Osti, "'So how do we balance all of these needs?': How the concept of AI technology impacts digital archival expertise," *Journal of Documentation*, vol. 79, no. 7, pp. 12–29, 2023, doi: 10.1108/JD-08-2022-0170.
- [4] A. U. Desai, "A review of the applications of machine learning in cybersecurity and its challenges," *Journal of Digital Security and Forensics*, vol. 1, no. 1, 2024, doi: 10.29121/digisecforensics.v1.i1.2024.17.
- [5] L. Han et al., "Power load forecast based on CS-LSTM neural network," *Mathematics*, vol. 12, no. 9, p. 1402, 2024, doi: 10.3390/math12091402.
- [6] J. Kim et al., "Key backup and recovery for resilient DID environment," *Mathematics*, vol. 12, no. 6, p. 830, 2024, doi: 10.3390/math12060830.
- [7] N. B. Malvi et al., "Sustainable data storage solutions using AI," in *Proceedings of a Scientific Conference on Data Technologies*, 2025, pp. 321–340.
- [8] McKinsey Global Institute, *The State of AI in 2019*. McKinsey & Company, 2019.
- [9] T. Mehra, "AI-driven approach to advancing backup strategies and optimizing storage solutions," *International Journal of Scientific Research in Engineering and Management*, vol. 8, no. 12, pp. 1–7, 2024, doi: 10.55041/IJSREM39778.
- [10] T. Mehra, "Building a resilient backup infrastructure: Combining data redundancy, encryption, and RBAC for maximum protection," *International Journal of Scientific Research in Engineering and Management*, vol. 9, no. 3, pp. 1–9, 2025, doi: 10.55041/IJSREM41975.
- [11] E. E. S. Murphy and J. D. Mehr, "Intelligent tiers of backup data," U.S. Patent EP2422274B1, May 6, 2020. [Online]. Available: <https://data.epo.org/publication-server/rest/v1.2/publication-dates/20200506/patents/EP2422274NWB1/document.html>
- [12] P. Novak et al., "Multistage malware detection method for backup systems," *Technologies*, vol. 12, no. 2, p. 23, 2024, doi: 10.3390/technologies12020023.
- [13] L. Peng et al., "SecDedup: Secure data deduplication with dynamic auditing in the cloud," *Information Sciences*, vol. 644, p. 119279, 2023, doi: 10.1016/j.ins.2023.119279.
- [14] N. Saad, N. Elmqaddem, and E. Vasseur, "Artificial intelligence at the service of digital archiving: Optimization of practices and ethical challenges," 2022.
- [15] A. Sghir et al., "Advanced strategies for big data resource and storage optimization: An AI perspective," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 8, 2025, doi: 10.14569/IJACSA.2025.0160896.
- [16] D. Shailesh et al., "Systems and methods for prioritizing and detecting file datasets based on metadata," U.S. Patent US11487825B1, 2022. [Online]. Available: <https://patentimages.storage.googleapis.com/76/24/01/d500122b6890c1/US11487825.pdf>
- [17] A. Chagovec, T. Bakardjieva, A. Ivanova, F. Sapundzhi, V. Spasova, and A. Ivanova, "AI-driven threat detection and automated incident response for securing cloud workloads," in *Proceedings of the 6th International Electronic Conference on Applied Sciences*, MDPI, Basel, Switzerland, Dec. 9–11, 2025. [Online]. Available: <https://sciforum.net/paper/view/27875>
- [18] AI-Driven Autonomous Backup Systems for Proactive Disaster Recovery in Cloud Environments," *Budapest Journal of Computational Intelligence and Robotics*, vol. 6, pp. 1–9, 2022
- [19] Karthick R., "Advanced Threat Detection in Backup Systems: AI, Encryption, and RBAC," *ESP Journal of Engineering Technology Advancements*, ICECT 2024.
- [20] Microsoft, "SCI XDR Ebook: Supercharge your security operations with XDR," Microsoft Security, 2022.
- [21] R. Thomas and S. A. Fathima, "AI-Based Backup Security Solutions: Detecting Anomalous Activities and Strengthening Encryption," *International Journal of Multidisciplinary on Science and Management*, ICETETI 2024, pp. 174–179.
- [22] StoneFly Inc., "Threat Detection, Monitoring, and Ransomware Protection with AI-Based XDR and SIEM Platform," *PRWeb*, May 2025.
- [23] A. Author et al., "ZADIG: A Novel Extended Detection and Response System," *IEEE Xplore*, 2025.

Automated Vulnerability Assessment in Windows Active Directory and Oracle Database Environments using PowerShell and SQL*Plus

Vasil Slavyanov
PhD Student
Vasil Levski National Military
University
Veliko Tarnovo, Bulgaria
vasil.slavyanov@gmail.com

Abstract—Enterprise IT environments are rarely built around a single technology. In most mid-to-large organisations, identity management runs through Microsoft Active Directory while business-critical data sits in relational databases such as Oracle. This combination is operationally essential and a recurring focus of security incidents. Reviewing such environments manually is slow, inconsistent across reviewers, and leaves real gaps in coverage. This paper describes a practical approach to automating vulnerability assessment across both layers using tools already present in the environment: PowerShell for the Windows and Active Directory side, and SQL*Plus for Oracle Database. The focus is on configuration weaknesses, access control gaps, and governance failures that accumulate quietly in production systems. The paper presents a methodology, discussion of typical findings, and an honest account of where the approach runs into its limits.

Keywords— Active Directory, configuration auditing, internal control testing, Oracle Database, PowerShell, security automation, SQL*Plus, vulnerability assessment

I. INTRODUCTION

Security problems in enterprise environments tend not to arrive through the front door. They accumulate — in stale accounts, overpermissioned service users, password policies that were never enforced, audit settings that were configured once and never revisited. The gap between what an organisation's policy documents say and what is actually running in production is often wider than anyone realises, and it is rarely visible without looking directly at the technical configuration.

Active Directory and Oracle Database together represent a substantial portion of the attack surface in most enterprise environments. Active Directory controls who can authenticate, what they can access, and which policies apply to which systems. Oracle Database holds the data that organisations are most likely to be contractually and legally obligated to protect. Weaknesses in either layer carry

serious consequences; weaknesses in both, which is common, compound each other.

The conventional approach to reviewing these environments relies heavily on the knowledge and diligence of whoever conducts the review. A reviewer who knows what to look for in Active Directory may know considerably less about Oracle, and vice versa. Even where competence is not an issue, manual review is slow, and a slow process tends to get compressed or skipped when audit timelines tighten.

Automation addresses the most persistent part of the problem: whether the data was actually collected, consistently, in a form that can be reviewed. PowerShell and SQL*Plus are available in any domain-joined Windows environment and any Oracle installation. Using them systematically produces a complete, comparable, timestamped picture of what the environment actually looks like.

Section 2 establishes the problem context; Section 3 describes the methodology. The Active Directory and Oracle assessment layers are treated in Sections 4 and 5 respectively. Section 6 characterises typical findings, Section 7 examines limitations, Section 8 addresses practical application within audit and compliance contexts, and Section 9 concludes

II. PROBLEM STATEMENT AND MOTIVATION

This paper addresses a specific kind of problem: not zero-days or sophisticated exploitation techniques, but the mundane security failures that cause the most damage in enterprise environments. A domain administrator account belonging to an employee who left three years ago. A service account with DBA rights that nobody remembers creating. A password policy applied to ninety percent of users but not the accounts that actually matter. These are

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.146>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

configuration and governance failures, and they persist because nobody looks for them systematically.

Active Directory is a particularly productive source of this kind of problem. Because it underpins authentication and policy enforcement across the entire domain, a misconfiguration does not stay local — it propagates. Mokhtar et al. [7] point out that the breadth of adoption of Active Directory services has made them a consistent target, and that attack techniques have evolved specifically to exploit misconfigurations in group memberships, delegation settings, and authentication configurations.

The Oracle Database side of the problem is similar in origin. Database environments tend to accumulate excessive privilege over time as application requirements change, developers request access and move on, and DBAs apply workarounds that remain in place long after the original problem is resolved. Omotunde and Ahmed [8] identify improper access control enforcement as among the primary contributors to database security incidents in contemporary organisations.

Three practical requirements follow. First, assessment needs to be repeatable. Second, the evidence needs to be defensible — findings based on structured script output tied to specific configuration objects are not easily challenged. Third, the process needs to be efficient enough to actually happen within normal audit planning constraints.

III. METHODOLOGY

The methodology is built around four principles that reflect deliberate choices about what kind of assessment this is.

3.1 Assessment Principles

The first principle is to use only what is already there. PowerShell and SQL*Plus are available in any environment where Windows and Oracle are deployed. Scripts based on native capabilities avoid deployment friction and questions about authorisation.

The second principle is read-only operation. Nothing in the assessment modifies the target environment. This is non-negotiable for any review conducted in a production context, and it is what separates a configuration assessment from a penetration test.

The third principle is control orientation. The scripts are structured to answer specific questions: is this setting within the range the policy requires? Does this account have attributes that should have triggered a review? Are these group memberships consistent with the documented access model?

The fourth principle is structured output. Results are exported in formats — CSV, JSON, or timestamped text — that can be reviewed by a human, processed analytically, and stored as audit evidence.

3.2 Assessment Stages

Stage 1: Scope Definition

Before any script runs, the reviewer defines what is in scope: which domains, which domain controllers, which

member servers, which Oracle instances. Scope decisions determine what the assessment can and cannot conclude, and an ambiguous scope is a common reason why findings get disputed after the fact.

Stage 2: Automated Data Collection

Scripts are executed against the defined scope to extract configuration data. For Active Directory and Windows, this covers user and group objects, Group Policy settings, local administrator membership, installed roles, open ports, running services, event log configuration, and registry-based security parameters. For Oracle, it covers user account status, role and privilege assignments, profile settings, password controls, and audit configuration.

Stage 3: Control Evaluation

The collected data is reviewed against control expectations. Some evaluations can be automated — accounts inactive for more than ninety days, passwords set to never expire, users with DBA role. Others require human judgement — whether a particular group membership is justified, whether a deviation from password policy is covered by a documented exception.

Stage 4: Reporting and Follow-Up

Findings are documented with a description of what was observed, a statement of why it matters, the specific evidence that supports it, and a recommendation. Technical outputs are attached as appendices. The whole package supports both management reporting and remediation tracking.

3.3 Evaluation Dimensions

Across both layers, assessment logic is organised around the same dimensions: identity and access management; privilege management; authentication and password controls; configuration hardening; logging and monitoring; audit readiness; and policy consistency across systems.

IV. AUTOMATED ASSESSMENT OF WINDOWS ACTIVE DIRECTORY AND SERVER ENVIRONMENTS

PowerShell's usefulness comes from the breadth of what it can reach. A single script, run from a domain-joined machine with appropriate read permissions, can enumerate user and group objects across the entire directory, pull Group Policy Object settings, query local configuration on individual servers, and export the results to structured files — all without installing anything, without modifying anything, and without requiring administrator cooperation.

4.1 Data Sources and Collection Areas

4.1.1 User Accounts

User account data is where most Active Directory assessments find their first substantive problems. The relevant attributes are enabled status, password last set date, last logon timestamp, whether the account has a non-expiring password, and whether it carries any administrative group membership. From these, it is possible to identify accounts not used in months but remaining enabled, accounts whose passwords have not changed in years, and service accounts that have

accumulated group memberships beyond what any documented role would justify.

4.1.2 Group Membership and Privilege Exposure

Privileged group membership in Active Directory — Domain Admins, Enterprise Admins, Account Operators, Backup Operators — deserves more scrutiny than it typically receives. Bu Haimed et al. [9] show experimentally that even modest initial access rights can be escalated to full domain administrative control when group and delegation configurations contain the kinds of misconfiguration that automated review is well placed to detect.

4.1.3 Organisational Units and Delegation

Delegation settings in the organisational unit structure are a less commonly reviewed area but can carry significant risk. Permissions delegated at the OU level for helpdesk workflows, password resets, or computer account management can, if misconfigured, provide pathways to privilege that bypass the standard administrative groups entirely.

4.1.4 Group Policy Objects

Group Policy is where the security baseline is supposed to live. The relevant settings — password and lockout policy, audit configuration, user rights assignment, local administrator control, remote access restrictions — are the documented intent of whoever designed the security architecture. The automated review extracts the actual GPO configuration and checks it against that intent. In practice, the two are frequently inconsistent.

4.1.5 Local Server Configuration

The local Administrators group on individual servers is particularly worth examining: it is not uncommon to find it containing individual user accounts added during incidents, test accounts never removed, or service accounts whose presence was never intended. Beyond group membership, the review covers running services, listening ports, firewall configuration, and event log settings.

4.2 Sample Assessment Logic

The following checks represent a practical starting set: identifying enabled accounts inactive beyond a defined threshold; listing accounts with non-expiring passwords; extracting and resolving nested membership of all privileged groups; comparing the effective domain password policy against documented requirements; identifying services running under privileged domain accounts; and verifying that audit policy configuration is centrally managed and complete.

4.3 Evidence and Output Structure

Each script output should carry at minimum a timestamp, a scope identifier, and a reference to the module or query that produced it. CSV is usually the most practical format for Active Directory exports. The discipline of saving outputs systematically — rather than reviewing them interactively and discarding them — is what makes it possible to produce defensible findings rather than recollections.

V. AUTOMATED ASSESSMENT OF ORACLE DATABASE ENVIRONMENTS USING SQL*PLUS

Oracle Database assessment through SQL*Plus works on the same principle: use what is already there, read only, compare against expected controls. The data dictionary views exposed through SQL*Plus provide access to everything a security reviewer needs — user account status, privilege and role assignments, profile settings, audit configuration — without requiring additional tooling and without leaving a footprint beyond the query itself in the audit log.

5.1 Security-Relevant Review Areas

5.1.1 Database Users and Account Status

The user inventory is the natural starting point. Which accounts are open, which are locked, which have never logged in recently, which are default Oracle accounts not secured at installation, and which application or service accounts lack an identifiable owner. An account with DBA privileges attached to an application decommissioned two years ago represents a real exposure, not a theoretical one.

5.1.2 Roles and Privileges

Privilege accumulation in Oracle environments follows a recognisable pattern. The DBA role gets assigned during a project because someone needed broad access temporarily and is never removed. A developer gets GRANT ANY PRIVILEGE during testing and the account is kept for support purposes. In aggregate, these describe a database where the privilege model provides very little actual constraint.

5.1.3 Profiles and Password Controls

Oracle profiles control password lifetime, reuse restrictions, failed login limits, and session timeout behaviour. The DEFAULT profile often retains its out-of-box settings — UNLIMITED password lifetime, no lockout after failed attempts, no verification function — long after it should have been hardened. Checking which accounts are on which profile, and what those profiles actually specify, is a straightforward query that frequently produces findings of immediate practical significance.

5.1.4 Audit and Logging Configuration

Database auditing is where Oracle assessments most consistently find problems. The question is not merely whether auditing is enabled — it is whether it captures the actions that would matter in an incident investigation: privileged user activity, DDL on sensitive objects, logon failures, modifications to audit configuration itself. An audit trail that records SELECT on a lookup table but not GRANT ANY PRIVILEGE is not providing meaningful assurance.

5.1.5 Configuration Review and Exposure Indicators

Beyond users and privileges, configuration parameters and structural features can increase exposure. Public synonyms that expose internal objects to any authenticated user, external procedure configurations, and initialisation parameters that weaken access enforcement are all worth checking.

5.2 Assessment Questions and Query Logic

The SQL*Plus queries are structured around specific questions rather than generic data dumps: which users have system privileges granted directly rather than through roles? Which accounts are in OPEN status but have not authenticated in the last ninety days? Which profiles have no failed login limit or no password verification function? Framing the queries this way produces output that maps directly to findings.

5.3 Assessment Value in the Audit Context

The practical benefit in audit terms is independence. When a finding is based on SQL*Plus output that the reviewer ran themselves against the production database, it is not dependent on what an administrator chose to show during a demonstration. It can be re-run to verify that remediation was applied. It can be compared against last year's output to show that a problem is not new.

VI. TYPICAL FINDINGS AND REPORTING MODEL

The findings that emerge from this kind of assessment are not surprising in type, but their prevalence usually is. Organisations that believe their access governance is broadly in order tend to discover, when they look at the actual configuration data, that the gap between policy and practice is substantially larger than expected.

6.1 Common Findings in Active Directory and Windows Environments

- Privileged groups contain accounts that cannot be justified against current role assignments, often because the access was granted for a specific purpose and never removed.
- Accounts remain enabled well past any reasonable inactivity threshold, including accounts belonging to former employees.
- The effective password policy, once GPO inheritance is resolved, applies weaker controls to certain account types than the documented policy specifies.
- Fine-grained password policies, where they exist, are applied inconsistently or to groups that do not reflect current account classification.
- Local Administrators group membership on servers has drifted from any documented baseline and is not periodically reviewed.
- Audit policy configuration is incomplete, often because it was set at domain level but overridden by local policy on critical servers.
- Service accounts carry privileges inherited from earlier configurations and have no documented owner accountable for reviewing them.

6.2 Common Findings in Oracle Database Environments

- System privileges are assigned directly to users rather than through roles, in quantities

that have no relationship to current operational requirements.

- Application and service accounts lack an identifiable owner and in some cases are associated with applications that no longer exist.
- The DEFAULT profile applies to accounts that should be on a more restrictive profile, and the DEFAULT profile itself retains weak or unlimited settings.
- DBA role assignments are broader than current operational needs.
- Audit configuration does not capture the actions needed to reconstruct a security incident.
- Privilege combinations exist that effectively bypass separation of duties in ways not reflected in any risk register or compensating control documentation.

6.3 Reporting Structure

The output from this assessment is structured as four components. An executive summary provides an overall picture of risk exposure, key themes across findings, and priority actions. A findings register documents each observation with a description of what was found, the risk it represents, evidence that supports it, and a specific recommendation. Technical appendices attach the structured script and query outputs. A remediation tracker assigns ownership, target dates, and a mechanism for follow-up verification.

VII. BENEFITS AND LIMITATIONS

7.1 Benefits

The most significant benefit is that the assessment actually gets done, consistently, across the full scope, every time it runs. Manual reviews tend to compress under time pressure, focus on systems where the reviewer has the most knowledge, and produce varying output depending on who conducts them. Scripts do not have these properties.

The cost profile is also worth noting. Once scripts are built and the reporting structure established, the marginal cost of running an assessment is low — lower than the equivalent manual review by a considerable margin — and the output is more complete and consistent.

7.2 Limitations

The most fundamental limitation is that this approach finds what it looks for. A script that checks password policy settings will find password policy problems. It will not find a social engineering attack in progress or a compromised credential being used within normal parameters. This is a configuration assessment, not threat detection.

The second significant limitation is interpretation. Automated extraction produces data; it does not produce judgement. Whether a particular group membership is justified, whether a deviation from password policy is

covered by a documented exception — these questions cannot be answered by a script.

There is also the maintenance question. Environments change, and scripts that are not updated will eventually produce incorrect or misleading output. Scripts should be treated as assets that require the same kind of lifecycle management as the controls they are designed to assess.

VIII. PRACTICAL APPLICATION IN INTERNAL AUDIT AND COMPLIANCE

Internal audit is the context where this approach delivers the most immediate practical value. Audit teams working in regulated environments are expected to provide assurance over access governance, privilege management, and configuration controls — often across multiple systems, within a constrained timeline, with findings that will be scrutinised by external reviewers and potentially by regulators.

Embedding automated extraction into the audit workflow changes the nature of the audit engagement. When an auditor arrives at an interview already holding structured data about the actual configuration, the conversation is different. The system owner cannot simply describe how the controls work in principle; they have to account for what the data shows. Findings based on script output are harder to dismiss and easier to track through to closure.

Beyond internal audit, the same methodology supports compliance work more broadly — regulatory reviews, third-party assessments, and continuous control monitoring programmes. The evidence requirements differ across these contexts but the underlying need — structured, traceable, reproducible technical data — is consistent.

IX. CONCLUSION

The argument of this paper is straightforward: configuration and governance weaknesses in Active Directory and Oracle Database environments are common, consequential, and largely invisible without systematic technical review. Manual review is insufficient to provide that visibility at the scale and consistency that regulated environments require. Automation using PowerShell and SQL*Plus can provide it, at a cost substantially lower than

the equivalent manual effort and with output that is more useful as audit evidence.

The methodology described here is not a replacement for professional judgement or for the broader suite of security testing tools that a mature security programme would employ. It is a foundation: a systematic way of ensuring that the basic configuration data is collected, consistently, in a form that supports both operational decision-making and audit assurance. In environments where that foundation does not currently exist, establishing it produces immediate and tangible improvement in security visibility.

Future development might productively focus on automated comparison of results against documented baselines, scoring mechanisms that weight findings by organisational context rather than just technical severity, and integration with continuous monitoring infrastructure.

REFERENCES

- [1] Microsoft Corporation. Windows Server and Active Directory documentation. Microsoft Docs. <https://docs.microsoft.com>
- [2] Oracle Corporation. Oracle Database Security Guide. Oracle Documentation. <https://docs.oracle.com/en/database/oracle/oracle-database/>
- [3] Center for Internet Security (CIS). CIS Benchmarks for Microsoft Windows Server and Oracle Database. <https://www.cisecurity.org>
- [4] ISACA. IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 4th Edition. ISACA, 2020.
- [5] NIST. Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [6] The Institute of Internal Auditors. International Standards for the Professional Practice of Internal Auditing. IIA, 2017.
- [7] Mokhtar, B. I., Jurcut, A. D., ElSayed, M. S., & Azer, M. A. (2022). Active Directory Attacks: Steps, Types, and Signatures. *Electronics*, 11(16), 2629. <https://doi.org/10.3390/electronics11162629>
- [8] Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems. *Mesopotamian Journal of CyberSecurity*, 2023, 115-133. <https://doi.org/10.58496/MJCSC/2023/016>
- [9] Bu Haimed, I., Albahar, M., & Alzubaidi, A. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks. *Future Internet*, 15(7), 226. <https://doi.org/10.3390/fi15070226>

Computer Vision Approach for Panorama Creation in Military Observation

Krasimir Slavyanov

Department Computer Systems and Technologies

Vasil Levski National Military University

Shumen, Bulgaria

k.slavyanov@nvu.bg

Abstract—In this paper the problem of obtaining a complete picture of monitored military objects is resolved with computer vision tools. The research is focused on the necessity for the correct arrangement of photos obtained in different ways to promptly obtain a comprehensive picture of the situation in an area of monitored military operation. The consecutive stages with functional operations are designed in MATLAB environment. Creation of a dataset with detailed images of specific zone of a military operation is described. Speeded-up robust features point detection is followed by descriptor extraction, transformation calculation and other specific computer vision tools. The functions for alpha blending and automatic black edge cropping are implemented for the final panorama creation.

Keywords— computer vision, panorama creation, speeded-up robust features, transformation calculation

I. INTRODUCTION

This document provides instructions for panorama creation in military observation. For the military reconnaissance operations, it is commonly popular to have a bunch of pictures derived by drone camera or some hidden stationary camera used to make several captures from one point of view. An approach with multiple viewpoint can also be implemented [1], [2]. To analyze whole picture of the observed military objects with their motion and arrangements approaching any possible future status or activity the panorama view is most valued and can be used easier for whole unit's status information analysis. The lower computational burden and faster processing speed, which can meet the real-time requirements for scene matching like in [3] are also valued in this approach. The speeded-up robust features (SURF) are implemented in this approach. SURF is very popular in different approaches for panorama creation [4] and multi-view image registration like in [5],[6] and can be improved in different ways [7],[8],[9],[10].

The implementation of the spatial orientation approach and the precise local positioning approach like in [11] can

also be implemented for calculation of the exact time for the photo capturing. Essential for the military reconnaissance, this approach for panorama creation can be used for other implementations where wider observation picture should be created like for agriculture purposes [12].

II. MATERIALS AND METHODS

To obtain a complete picture of monitored military objects, it is necessary to correctly arrange photos obtained in different ways to promptly obtain a comprehensive picture of the situation in the area of monitored military operation.

Panoramic images allow several photos to be combined into one whole image with a wide viewing angle. In the present scenario, a system for automatic panorama creation using the SURF (Speeded-Up Robust Features) method is implemented, using only classical computer vision techniques, without neural networks.

The first stage in the creation of panorama is the creation of a dataset with detailed images of specific zone of a military operation (status). Images can be obtained from a ground camera, a drone camera, or images generated by artificial intelligence, in which one or more military objects are captured. For the research purpose such a dataset is created and displayed on fig.1.



a) Image 1

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.153>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



b) Image 2



c) Image 3



d) Image 4



e) Image 5



f) Image 6

Fig. 1. A dataset with 6 images of observed military objects.

On the second stage calculations for each pair of images are performed. The images should be selected at first and then put in alphabetical order to follow their automatically generated by the camera firmware timestamp. The experiment is carried out in the MATLAB environment as follows:

A. User selection of images

An array is created with the filenames and their corresponding path names in the memory directory. The function *uigetfile* is used with the supporting functions for the file type check like *isequal* and *ischar*. Sorting in alphabetical order is the next step here. Variables are created for the full paths, images and their numbers [13].

```
[fileNames, pathName] =
uigetfile({'*.jpg;*.png;*.jpeg;*.bmp'
,
'Image Files (*.jpg, *.png,
*.jpeg, *.bmp)'}, ...
'Select images to create a
panorama', ...
'MultiSelect', 'on');
if isequal(fileNames, 0)
error('No images selected.');
```

Sorting in alphabetical order:

```
fileNames = sort(fileNames);
```

Creation of full paths, datastore:

```
fullPaths = fullfile(pathName,
fileNames);
images = imageDatastore(fullPaths);
numImages = numel(images.Files);
```

B. Loading the first image

The following steps on this stage are loading the first image and the detection and matching with the rest of the images from selection. These are carried out with the color to gray transform (function *im2gray*) and creation of variables for the picture size and for the homogeneous transformation matrix (function *projective2d*).

```
I = readimage(images, 1);
grayImage = im2gray(I);
imageSize = size(grayImage);
tforms(numImages) =
projective2d(eye(3));
```

C. Detection and matching with the rest of the images from selection

A simple *For* cycle is used for detection and matching with the rest of the images from selection.

```
for n = 2:numImages
% previous image
I1 = im2gray(readimage(images, n -
1));
I2 = im2gray(readimage(images, n));
%continues...
```

D. SURF features detection and processing

Next step on the second stage is the detection of the speeded-up robust features of the pictures in grayscale. *detectSURFFeatures* is a MATLAB function for finding the blob features. Description: `points = detectSURFFeatures(I)` returns a SURFPoints object, points, containing information about SURF features detected in the 2-D grayscale or binary input image I. This and the rest of the MATLAB functions can be found explained in the MATLAB documentation [13]:

```
% ... continued cycle:
% SURF features detection
points1 = detectSURFFeatures(I1);
points2 = detectSURFFeatures(I2);
[features1, validPoints1] =
extractFeatures(I1, points1);
[features2, validPoints2] =
extractFeatures(I2, points2);
indexPairs = matchFeatures(features2,
features1, 'Unique', true);
matchedPoints2 =
validPoints2(indexPairs(:,1), :);
matchedPoints1 =
validPoints1(indexPairs(:,2), :);
fprintf('Image %d: matches found =
%d\n', n, size(indexPairs,1));
if size(indexPairs,1) < 10
warning('Not enough matches
between images %d and %d. Skip.', n-
1, n);
tforms(n) =
projective2d(tforms(n-1).T);
continue;
end
```

E. Calculation of design transformation.

The function *estimateGeometricTransform2D* is used to estimate a 2-D geometric transformation between two images by mapping the inliers in the matched points from one image *matchedPoints1* to the inliers in the matched points from another image *matchedPoints2* [13].

```
tform =
estimateGeometricTransform2D(matchedP
oints2, matchedPoints1, ...
'projective', 'Confidence',
99.9, 'MaxNumTrials', 2000);

tforms(n).T = tform.T * tforms(n-
1).T;
```

F. Show the transformation matrix

```
disp(['T matrix of an image',
num2str(n), ':']);
disp(tforms(n).T);
```

The results here are the matrices of values:

Image 2: matches found = 6721
 T matrix of an image2:
 0.8710 -0.0085 -0.0000
 0.0577 0.9349 0.0000
 446.2032 14.0935 1.0000

Image 3: matches found = 6574
 T matrix of an image3:
 0.7816 -0.0034 -0.0000
 0.1300 0.8966 0.0000
 828.5522 4.7152 0.9880

Image 4: matches found = 3578
 T matrix of an image4:
 1.0e+03 *
 0.0007 0.0000 -0.0000
 0.0002 0.0008 0.0000
 1.2649 -0.0351 0.0010

Image 5: matches found = 2381
 T matrix of an image5:
 1.0e+03 *
 0.0005 0.0000 -0.0000
 0.0003 0.0008 0.0000
 1.7456 -0.0498 0.0009

Image 6: matches found = 1982
 T matrix of an image6:
 1.0e+03 *
 0.0004 0.0000 -0.0000
 0.0004 0.0007 0.0000
 2.0979 -0.1392 0.0008

G. Match preview

The function *showMatchedFeatures* [13] is used for the preview

```
figure;
showMatchedFeatures(I2, I1,
matchedPoints2, matchedPoints1,
'montage');
title(['matches between image ',
num2str(n-1), ' and ', num2str(n)]);
pause(1); % short break for
review
```

The matched SURF features are displayed on fig. 2.

Centering to the middle image and calculating panorama dimensions are the next steps evaluated for the panorama creation process.

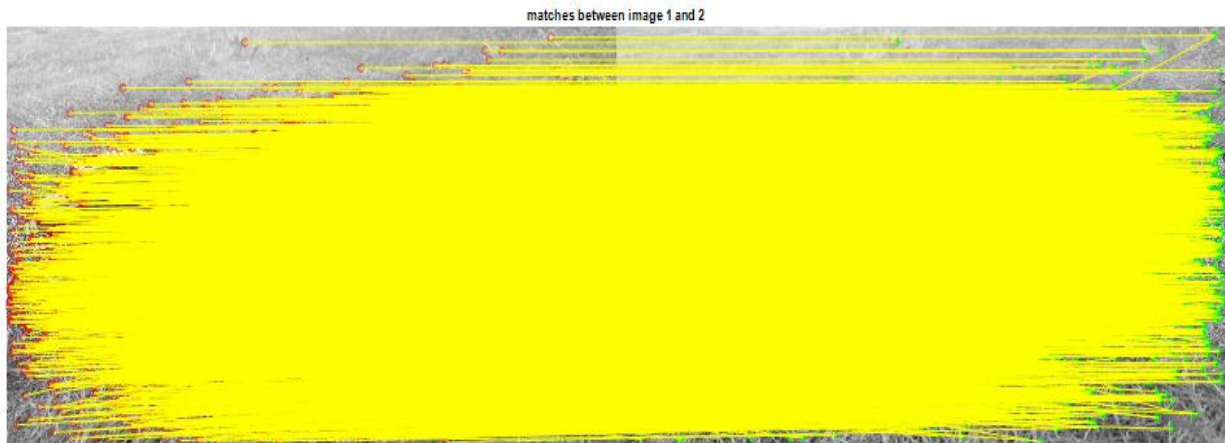


Fig. 2. Matched SURF features between the selected images (shown only between image 1 and image 2)

```
panorama = zeros([height width 3],
    'like', I);
blender =
    vision.AlphaBlender('Operation',
        'Binary mask', ...
        'MaskSource', 'Input port');

for i = 1:numImages

    I = readimage(images, i);
    warpedImage = imwarp(I,
        tforms(i), 'OutputView',
        panoramaView);
    mask = imwarp(true(size(I,1),
        size(I,2)), tforms(i), 'OutputView',
        panoramaView);
    panorama = step(blender,
        panorama, warpedImage, mask);
    fprintf('Added image %d to the
        panorama.\n', i);

end
```

```
minRow = min(row); maxRow =
    max(row);
minCol = min(col); maxCol =
    max(col);
croppedPanorama =
    imcrop(panorama, [minCol, minRow,
        maxCol-minCol, maxRow-minRow]);
else

    croppedPanorama = panorama; %
    fallback

end
```

III. RESULTS AND DISCUSSION

For the result showing the MATLAB can easily produce an image of the cropped panorama generated with the code explained above:

```
figure;
imshow(croppedPanorama);
title('Final panorama (cropped and
    improved)');
```

H. Automatic black edge cropping.

The *Imcrop* function used on this stage is an interactive Crop Image tool used to crop the grayscale, truecolor, or binary image displayed in the current figure. *imcrop* returns the cropped image, *Icropped* [13].

```
grayPanorama = rgb2gray(panorama);
mask = grayPanorama > 0;

[row, col] = find(mask);

if ~isempty(row) && ~isempty(col)
```

For better applicability of the approach, a small but accurate set of captured images of the required quality is required, which must be taken from a properly selected observation point that tracks the movement of objects.

As is described before, even a simple camera can be sufficient for panorama creation. Another implementation of computer vision can be applied afterwards for the military object detection purpose.

The algorithm described can be fruitful for panorama creation even if very detailed pictures are used and as can

be seen the environment is also very detailed. The Panorama view created is shown of fig. 3.



Fig. 3. Panorama view of the observed military objects.

IV. CONCLUSIONS

A common task during reconnaissance missions is to analyze whole picture of the observed military objects with their motion or their predicted arrangements in any possible future status or activity. Thus, the panorama view is most valued and can be used easier for whole unit's status information analysis.

Application creation using this algorithm can furthermore be elaborated where any other previous observation gathering information like predefined object searching or target acquisition can be also implemented for object detection after the panorama creation.

ACKNOWLEDGMENTS

This work was supported by the National Science Program "Security and Defence", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] G. Ramkumar, T. J. Nagalakshmi, N. Nalini, P. Jagadeesh, P. S. Bharathi and V. Amudha, "An Effective Construction of Multiple Viewpoint based Panorama Design using Digital Image Processing Scheme," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-6, <https://doi.org/10.1109/ACCAI53970.2022.9752626>.
- [2] S. Degadwala, U. Chakraborty, P. Kuri, H. Biswas, A. N. Ali and D. Vyas, "Real-Time Panorama and Image Stitching with Surf-Sift Features," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1111-1115, <https://doi.org/10.1109/ICICT50816.2021.9358586>.
- [3] Su Juan, Xu Qingsong and Zhu Jinghua, "A scene matching algorithm based on SURF feature," 2010 International Conference on Image Analysis and Signal Processing, Zhejiang, China, 2010, pp. 434-437, <https://ieeexplore.ieee.org/document/5476080>, <https://doi.org/10.1109/IASP.2010.5476080>.
- [4] Q. Fu and H. Wang, "A fast image stitching algorithm based on SURF," 2017 IEEE/CIC International Conference on Communications in China (ICCC), Qingdao, China, 2017, pp. 1-4, <https://doi.org/10.1109/ICCCChina.2017.8330425>.
- [5] M. S. Patel, N. M. Patel and M. S. Holia, "Feature based multi-view image registration using SURF," 2015 International Symposium on Advanced Computing and Communication (ISACC), Silchar, India, 2015, pp. 213-218, <https://doi.org/10.1109/ISACC.2015.7377344>.
- [6] S. Ali and M. Hussain, "Panoramic image construction using feature based registration methods," 2012 15th International Multitopic Conference (INMIC), Islamabad, Pakistan, 2012, pp. 209-214, <https://doi.org/10.1109/INMIC.2012.6511464>.
- [7] Cai, P. Wang and Y. -h. Liang, "Fast image stitching based on improved SURF," 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanchang, China, 2016, pp. 411-416, <https://doi.org/10.1109/CSCWD.2016.7566024>.
- [8] X. Li, S. He, X. Gao and J. Zhou, "Research on Container Panorama Image Stitching Method," 2018 Chinese Automation Congress (CAC), Xi'an, China, 2018, pp. 661-664,

- <https://doi.org/10.1109/CAC.2018.8623589>.
- [9] L. Juan and G. Oubong, "SURF applied in panorama image stitching," *2010 2nd International Conference on Image Processing Theory, Tools and Applications*, Paris, France, 2010, pp. 495-499, <https://doi.org/10.1109/IPTA.2010.5586723>.
- [10] R. Monali, S. Moonka, A. Priya and S. S. Tripathy, "Effects of noise and relative overlap on image mosaicing using SURF features," *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2016, pp. 773-777, <https://doi.org/10.1109/RTEICT.2016.7807931>.
- [11] V. Atanasov, T. Trifonov, "A new model of ultra wideband sensors based interactive system", *International Journal on Information Technologies and Security*, № 1 (vol. 16), 2024, pp.39-48, ISSN 1313-8251, <https://doi.org/10.59035/XYCG3094>
- [12] M. Iliev and M. Bedzheva, "An Aproach for Application of UAVs for Observation of Processes in Agriculture", *7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE)*, 2020, <https://doi.org/10.1109/EEAE49144.2020.9279028>
- [13] <https://www.mathworks.com/help/matlab/index.html> [Accessed: Apr. 05, 2026].

A Computer Vision Approach to Military Object Recognition

Krasimir Slavyanov

Department Computer Systems and Technologies

Vasil Levski National Military University

Shumen, Bulgaria

k.slavyanov@nvu.bg

Abstract—This research described is focused on computer vision tools implemented for detection of a particular military object (or many objects) in a observed scene, given a reference image(s) of the object(s). An algorithm for detecting a specific object based on finding point correspondences between the reference and the target image is designed. It can detect objects despite a scale change or in-plane rotation. It is also robust to small amount of out-of-plane rotation and occlusion. Reference images and a dataset with images obtained from a ground camera are used for the experiments. Detection of point features in images and extraction of feature points are designed for Localization of the recognized object(s) in a scene using matches of feature points (groups of points).

Keywords — computer vision, military objects, reference images, speeded-up robust features

I. INTRODUCTION

The application of object detection and recognition provides the ability to recognize objects with their 2D positions in the image [1], [2]. Apart from machine learning approaches [3], deep learning [4] and neural network implementation [5], [6], this approach is solving the problem of how to detect a particular military object (or many objects) in a different operational environment, given a reference image(s) of the object(s) using only some common computer vision functions that can be found in the MATLAB. Local features and their descriptors, which are compact vector representations of the local environment, are the building blocks of many computer vision algorithms like Yolo for fast, accurate real-time object detection, segmentation, and classification [7], [8]. Their applications include image registration, object detection and classification, and motion tracking and estimation. The use of local features allows these algorithms to better cope with changes in scale, rotation, and occlusion. An algorithm for detecting a specific object based on finding point correspondences between the reference and the target image(photo) is presented. The implementation of the

spatial orientation approach and the precise local positioning approach like in [9] can be implemented for calculation of the exact time for the photo capture. The object detection in photos works best for objects that exhibit non-repeating texture patterns, which give rise to unique feature matches. This technique is not likely to work well for uniformly colored objects, or for objects containing repeated patterns.

The algorithm is designed for detecting specific military object(s), for example, military vehicles. Detectors that rely on gradient and intensity variation approaches detect contrasting local features. These features include edges, spots, and regions. The selected local features show repeatable detections. Given two images of the same scene, most of the features that the detector finds in both images are the same. The features are robust to changes in viewing conditions and noise. Even confidential information can be hidden in an image using steganographic approach [10].

Effective military object detection can handle different tactical scenes: changes to the object size, location, orientation, and other challenges. Computer Vision System Toolbox in MATLAB offers a variety of techniques for handling challenges in military object detection.

This approach example shows how to detect a particular object in a panorama scene, given a reference image of the military object – a vehicle. The example presents an algorithm for detecting a specific military object based on finding point correspondences between the reference and the target image. It can detect objects despite a scale change or in-plane rotation. It is also robust to small amounts of out-of-plane rotation and occlusion.

II. MATERIALS AND METHODS

For better understanding the research is structured in several stages, each with specific purpose.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.154>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

A. Create a dataset with detailed reference images of specific military vehicles

To detect a specific military vehicle(s) a dataset of reference images should be created (or later updated).

Creating a set of reference images allows the detection of a change in location or reappearance of military objects of interest.

An important condition is that military objects - vehicles - are captured with higher image quality (brightness, sharpness, contrast etc.). For that stage of the approach three well know vehicles are captured to produce the dataset of referent image – Land Rover Defender, High Mobility Multipurpose Wheeled Vehicle (HMMWV or more popular as Humvee), named here as humvee1 and another version of the HMMWV – humvee2, all shown on fig. 1.



a) Land Rover Defender



b) HMMWV – humvee1



c) HMMWV – humvee2

Fig. 1. Referent images of a military vehicles: Land Rover Defender, HMMWV – humvee1, HMMWV – humvee2.

B. Observation and photo capturing.

The main goal at this stage is the creation of a dataset with images obtained from a ground camera, a drone camera, or images generated by artificial intelligence, in

which one or more military vehicles are captured. A small set of complex images including more than one military vehicle is required.

The overall image can be with a scale change or in-plane rotation, with a small amount of out-of-plane rotation and occlusion. For that purpose, just one image out of the dataset is needed. One selection of all the mentioned before military vehicles is shown on fig.2.



Fig. 2. An image with some of the predefined military vehicles on the field - a target for the recognition process.

C. Read the reference image containing the object of interest

At this stage a reading of the target images is conducted in a MATLAB environment. Reading the reference image(s) containing the object of interest into MATLAB. The `rgb2gray` function is used for this purpose.

```
defenderImage =
imread('defender.jpg');
defenderImage =
rgb2gray(defenderImage);
figure;
imshow(defenderImage);
title('Image of Defender');
sceneImage = imread('vehicles.jpg');
sceneImage = rgb2gray(sceneImage);
figure;
imshow(sceneImage);
title('Image of a scene')
```

The images are converted from colored RGB type to greyscale images. The result for the Defender vehicle is shown on fig 3.



Fig. 3. A Greyscale reference image of Land Rover Defender

The greyscale image of the observation capture is on fig. 4.



Fig. 4. The observation capture in greyscale

D. Detect point features in both images

The function *detectSURFFeatures* for SURF (Speeded-Up Robust Features) method [11] is implemented, using only classical computer vision techniques, without neural networks. A variable is created with the result of the detection of characteristic points of the entire image (Defender).

```
defenderPoints =  
detectSURFFeatures(defenderImage);  
scenePoints =  
detectSURFFeatures(sceneImage);
```

Plotting the most contrasting 100 points carried out with the function *selectStrongest*. Visualization of the strongest features of the reference image is on fig. 5.

```
figure;  
imshow(defenderImage);  
title('100 Strongest Point Features  
from Defender Image');  
hold on;  
plot(selectStrongest(defenderPoints,  
100));
```



Fig. 5. Visualization of the strongest features of the reference image

Visualizing the strongest features of the target image (fig. 6):

```
figure;  
imshow(sceneImage);  
title('300 Strongest Point  
Features from scene Image');  
hold on;  
plot(selectStrongest(scenePoints,  
300));
```



Fig. 6. Strongest features of the target image

E. Extract feature points (groups of points) and find extracted matching features

The extraction of the features of the points of interest in both images is executed with the functions *extractFeatures*. The function *matchFeatures* is used for finding the putatively matching features(pairs).

```
[defenderFeatures, defenderPoints] =  
extractFeatures(defenderImage,  
defenderPoints);  
[sceneFeatures, scenePoints] =  
extractFeatures(sceneImage,  
scenePoints);  
defenderPairs =  
matchFeatures(defenderFeatures,  
sceneFeatures);
```

The creation of an image of the matched points is depicted on fig. 7.

```
matcheddefenderPoints =  
defenderPoints(defenderPairs(:, 1),  
:);  
matchedscenePoints =  
scenePoints(defenderPairs(:, 2), :);  
figure;  
showMatchedFeatures(defenderImage,  
sceneImage, matcheddefenderPoints,  
matchedscenePoints, 'montage');  
title('Putatively Matched Points  
(Including Outliers)');  
figure;  
showMatchedFeatures(defenderImage,  
sceneImage, matcheddefenderPoints,  
matchedscenePoints, 'montage');
```

```
title('Putatively Matched Points  
(Including Outliers)');
```

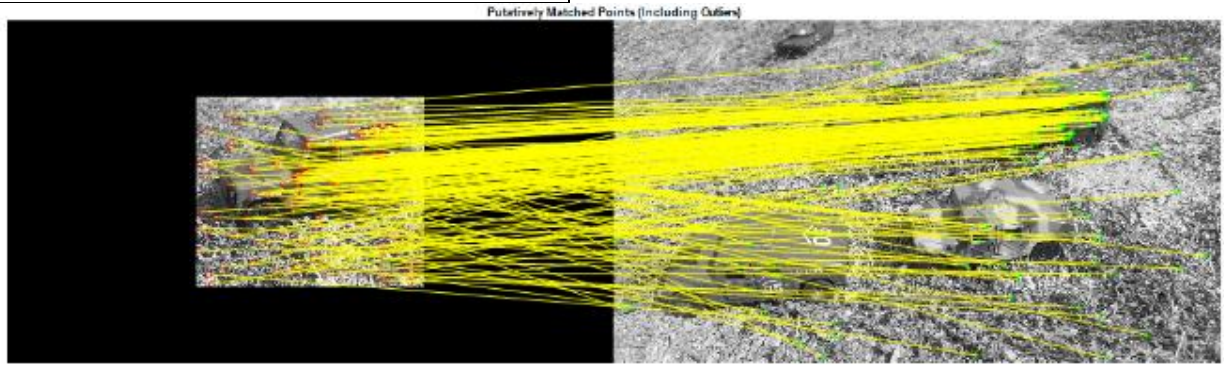


Fig. 7. Images of the matched points in the referent image and the captured image

F. Localization of the recognized object(s) in the scene using matches of feature points (groups of points).

At this stage a localization of the object in the scene is performed using presumed matches. The *estimateGeometricTransform* function is applied for the calculation of the transformation connecting the matching points while eliminating outliers. This transformation allows us to localize the object in the scene.

```
[tform, inlierdefenderPoints,  
inlierscenePoints] = ...  
estimateGeometricTransform(matchedde  
fenderPoints, matchedscenePoints,...  
'affine');
```

The matching pairs of points with outliers removed can then be displayed. The result of that procedure is depicted on fig. 8.

```
figure;  
showMatchedFeatures(defenderImage,  
sceneImage, inlierdefenderPoints,  
inlierscenePoints, 'montage');  
title('Matched Points (Inliers  
Only)');
```

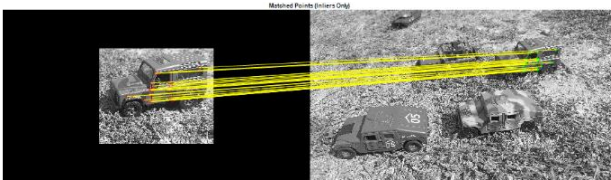


Fig. 8. The matching pairs of points with outliers removed for the recognized Land Rover Defender

A bounding polygon can then be formed around the recognized military vehicle:

```
defenderPolygon = [1, 1;... % up  
left
```

```
size(defenderImage, 2), 1;... % up  
right  
size(defenderImage, 2),  
size(defenderImage, 1);... % down  
right  
1, size(defenderImage, 1);... %  
down left  
1, 1]; % up left gain (closing)
```

To specify the location of the object in the scene, we can transform the polygon into the coordinate system of the target image (depicted on fig. 9):

```
newdefenderPolygon =  
transformPointsForward(tform,  
defenderPolygon);  
% creating figure  
figure;  
imshow(sceneImage);  
hold on;  
line(newdefenderPolygon(:, 1),  
newdefenderPolygon(:, 2), 'Color',  
'y', 'LineWidth', 3);  
title('Detected Defender');
```



Fig. 9. Bounding polygon formed around the recognized military vehicle

III. RESULTS AND DISCUSSION

Similarly, after the evaluation of the same six stages, the other objects in this photo (humvee1 and humvee2) can be found, and they are finally marked with a different color. The results from the recognition of humvee1 and humvee2 are represented on fig. 10 and fig. 11.

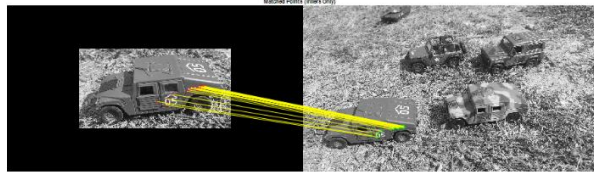


Fig. 10. The matching pairs of points with outliers removed for the recognized HUMVEE1

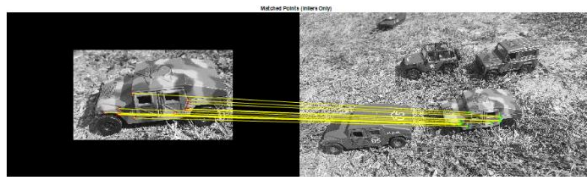


Fig. 11. The matching pairs of points with outliers removed for the recognized HUMVEE2

The three military vehicles can be recognized and then displayed on the target image with different colors – displayed on fig. 12.

```
figure;
imshow(sceneImage);
hold on;
line(newdefenderPolygon(:, 1),
newdefenderPolygon(:, 2), 'Color',
'y', 'LineWidth', 3);
line(newhumveePolygon(:, 1),
newhumveePolygon(:, 2), 'Color', 'b',
'LineWidth', 3);
line(newh2Polygon(:, 1),
newh2Polygon(:, 2), 'Color', 'r',
'LineWidth', 3);
title('Detected Defender, humvee 1
and humvee 2');
```

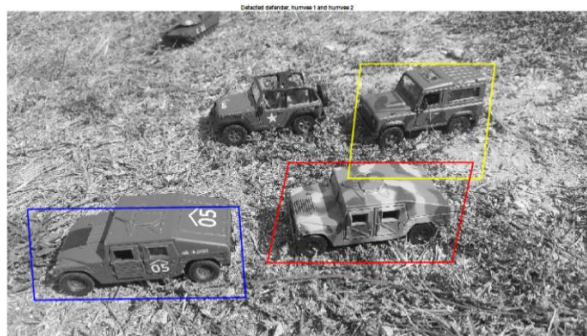


Fig. 12. The recognized Land Rover Defender, HUMVEE1 and HUMVEE2

IV. CONCLUSIONS

This approach of object detection works best for military objects that exhibit non-repeating texture patterns, which give rise to unique feature matches. This technique is not likely to work well for uniformly colored objects or for objects containing repeating patterns. Note that this algorithm is designed for detecting a military object, for example, well known military vehicles in reference images, rather than any vehicle. Computer vision recognition techniques can be used for clearly depicted and detailed objects. When recognizing partially hidden or significantly altered objects, better results could be obtained using artificial neural networks.

ACKNOWLEDGMENTS

This work was supported by the National Science Program "Security and Defence", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] H.Namdari, D.Nanda, X.Yuan, (2022). Progress in Computer Vision: Object Recognition. In: Albert, M.V., Lin, L., Spector, M.J., Dunn, L.S. (eds) Bridging Human Intelligence and Artificial Intelligence. Educational Communications and Technology: Issues and Innovations. Springer, Cham.
https://doi.org/10.1007/978-3-030-84729-6_5
- [2] M. Vashisht and B. Kumar, "A Survey Paper on Object Detection Methods in Image Processing," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-4,
<https://doi.org/10.1109/ICCSEA49143.2020.9132871>.
- [3] T. A. Nayeem, S. M. Motaharuzzaman, A. T. Hoque and M. H. Rahman, "Computer Vision Based Object Detection and Recognition System for Image Searching," 2022 12th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 2022, pp. 148-151,
<https://doi.org/10.1109/ICECE57408.2022.10089019>
- [4] I. Atik, "Deep Learning In Military Object Detection: An Example of The Yolo-Nas Model," 2024 8th International Symposium on Innovative Approaches in Smart Technologies (ISAS), İstanbul, Türkiye, 2024, pp. 1-7,
<https://doi.org/10.1109/ISAS64331.2024.10845459>.
- [5] J. Cherapanamjeri and B. N. K. Rao, "Neural Networks based Object Detection Techniques in Computer Vision," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 1092-1099,
<https://doi.org/10.1109/ICIRCA54612.2022.9985581>.
- [6] S. Kaushik, A. Raman and K. V. S. Rajeswara Rao, "Leveraging Computer Vision for Emergency Vehicle Detection-Implementation and Analysis," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6,
<https://doi.org/10.1109/ICCCNT49239.2020.9225331>
- [7] S. Singh and R. G N, "Military Based Object Detection in Satellite Imagery by Optimising YOLOv8," 2024 IEEE Space, Aerospace and Defence Conference (SPACE), Bangalore, India, 2024, pp. 165-168, <https://doi.org/10.1109/SPACE63117.2024.10667819>
- [8] S. Ali, Abdullah, A. Athar, M. Ali, A. Hussain and H. -C. Kim, "Computer Vision-Based Military Tank Recognition Using Object Detection Technique: An application of the YOLO Framework," 2023 1st International Conference on Advanced Innovations in

- Smart Cities (ICAISC), Jeddah, Saudi Arabia, 2023, pp. 1-6, <https://doi.org/10.1109/ICAISC56366.2023.10085552>
- [9] V. Atanasov, T. Trifonov, "A new model of ultra wideband sensors based interactive system", International Journal on Information Technologies and Security, № 1 (vol. 16), 2024, pp.39-48, ISSN 1313-8251, <https://doi.org/10.59035/XYCG3094>
- [10] V. Stoyanova, I.Lilov "Steganographic algorithm using the different color components of a 24-bit image", Security & Future, WEB ISSN 2535-082X; PRINT ISSN 2535-0668, Vol. 5 (2021), Issue 2, pg(s) 61-63
- [11] <https://www.mathworks.com/help/matlab/index.html> [Accessed: Apr. 05, 2026].

Designing a Firewall System for a Computer Network Based on a Single-Board Computer

Krasimir Slavyanov

Department Computer Systems and Technologies
“Vasil Levski” National Military University
Shumen, Bulgaria
k.o.slavyanov@gmail.com

Angela Borisova

Department Computer Systems and Technologies
“Vasil Levski” National Military University
Shumen, Bulgaria
angela.borisova@abv.bg

Abstract — When configuring temporary or hastily built, field or other computer networks, it is necessary that they meet all modern standards and requirements for computer networks and for cybersecurity when connecting to the Internet. This study proposes an approach for designing, configuring and setting up a firewall for a computer network, built and configured based on a Raspberry Pi single-board computer and free software. The basic configuration and operation with the various functionalities of the Intrusion Prevention System are described in detail. The application of the proposed solution is possible both for training and research in laboratory conditions and for permanent operation and monitoring of the system by specialists in real conditions and continuous operation.

Keywords — *firewall, intrusion prevention system, single-board computer*

I. INTRODUCTION

In many cases, when it is necessary to build a computer network, this may have to be done in a short time, without the necessary funding, due to logistical or other problems, and without the full set of necessary computer and network equipment that meets all the standards for this. Often, a temporary solution to the problem can turn out to be quite long. However, it is difficult to compromise with cybersecurity, especially if we are talking about small businesses with not many users and employees and, accordingly, with small computer networks and not so serious traffic, which also have to be analyzed in some cases for special or military operations [1]. Relatively cheap solutions can offer single-board computers such as Arduino, Raspberry Pi, etc. Especially Raspberry Pi boards have proven their effectiveness, both in managing the Internet of Things (IoT) [2], Web of Things [3] - smart home systems, IoT vulnerability analysis [4], managing physical security systems, controlling robots, drones, testing cybersecurity [5], VoIP [6], wireless network [7], [8] and unfortunately, they also turn out to be some of the most dangerous devices used by malicious users of a

computer network. Intrusion detection and alert supported by cloud solutions with Neural Networks is also an example of how efficient the single board computers can be [9].

This report proposes an easily feasible and sufficiently reliable solution to this problem, without investing significant financial resources, but providing basic security, firewall, gateway, router with basic capabilities. This is a computer system built based on a Raspberry Pi 4.0 single-board computer, functioning as a firewall. An open-source intrusion detection system (IDS) is designed and configured based on the IPFire firewall software.

II. MATERIALS AND METHODS

The following hardware is required for the system build: Raspberry Pi 4.0 (8 GB) with power supply, USB to Ethernet adapter – supporting 1000 Mbps (USB 3.0), micro SDXC memory card (min 32 GB), HDMI to micro-HDMI adapter, HDMI cable, HDMI monitor, USB keyboard.

The software required for the installation includes the following open-source products:

- Raspberry Pi Imager (ver.2.0.7)
- IPFire 2.29 core200 (ver. aarch64, “.xz” archive)

For better understanding the research is structured in several stages, each with specific purpose.

A. Flashing the memory with the IPFire OS

To flash the proper version of the ipfire OS, it should be downloaded from the official website of the company, in our case it is <https://www.ipfire.org>. The version of the software needed is ver. aarch64, an archive with extension “.xz” is needed.

An important condition is that the ipfire OS should be flashed on the memory card with the Raspberry Pi official software for that purpose - Raspberry Pi Imager, which should be downloaded also from the official website of the company <https://www.raspberrypi.com> with version proper for the Operational System of the computer used for the purpose. The experience in that stage proved that using another software for bootable storage creation like Rufus,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.171>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Balena Etcher etc. is not a working option. Just after the flashing procedure is completed and verified it is important to change the value of the parameter SERIAL-CONSOLE to OFF, the option is in the file uEnv.txt. The content of the file should look like this:

```
KVER=6.18.7-ipfire
root_dev=UUID=10114230-2832-4935-94ac-91a6b8e43be2
SERIAL-CONSOLE=OFF
```

B. Assembling and configuring the firewall system.

For the installation and configuration of the Raspberry Pi based firewall system, the previously flashed with the ipfire OS memory card should be installed on the board. For configuration access to the board, it should have a USB keyboard attached as well as some HDMI connected display. For the monitor it is important to be attached to the first micro-HDMI port (HDMI0, the left one), otherwise a rainbow colors will be displayed.

The additional USB to Ethernet adapter – supporting 1000 Mbps must be connected to one of the pair of USB 3.0 ports, where higher data transfer rate is supported.

The need of two ethernet RJ45 ports is essential because the firewall as it is by its purpose should have one port connected to the internet provider (WAN). This stream is called RED in the IPFire software. For the needs of the approach here RED connection will be configured to use the built-in RJ45 port. The LAN connection for the firewall is called GREEN, and it is planned to be configured on the additional USB 3.0 to Ethernet adapter.

After all the assembling is done before attaching the network cable the system has to be powered on and then configured with the following network properties for the installed IPFire operational system:

1. Language and time, according to the planned system operational location.
2. Machine host name, passwords for the users “root” and “admin”.
3. Selection of the network configuration type – there are several options according to the type of the service needed:
 - RED -as mentioned before is for the WAN
 - GREEN – for the LAN segment
 - BLUE for the local Wi-Fi network
 - ORANGE – for the DMZ (web servers, financial, HR or other functional system)

For the experiment only the basic configuration type is chosen RED + GREEN, as for the firewall use between WAN and LAN.

4. Drivers and card assignments – here the selection for the RED and the GREEN network adapter should be made, a variant is shown:

```
GREEN: "usb: Realtek Semiconductor
Corp. RTL8153 Gigabit Ethernet
Adapter"
GREEN: (fc: 19:28:66:f3:3c)
RED : "of: bcmgenet"
RED : (d8:3a:dd:f1:0b:d1) GREEN RED
```

5. IP Address settings for the RED and GREEN interface:

- The WAN interface (RED) in the most common case uses a DHCP service, therefore the configured settings are consistent with this., shown on fig. 1.

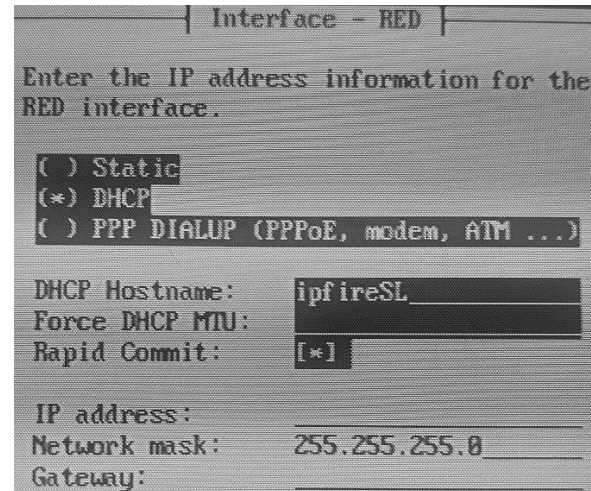


Fig. 1. Address settings for WAN (RED) interface.

- The IP address information for the LAN interface GREEN interface is configured as follows:

```
IP address:192.168.4.1
Network mask:255.255.255.0
```

The DHCP configuration is chosen to be as follows:

```
DHCP server configuration

Configure the DHCP server by
entering the settings information.

[*] Enabled

Start address:192.168.4.58
End address:192.168.4.254
Primary DNS:192.168.4.1
Secondary DNS:4.2.2.2.
Default lease (mins): 60
Max lease (mins):120
Domain name suffix: localdomain
```

C. Firewall Software configuration.

After the installation configuration the Raspberry Pi based firewall system should be connected as described before to the WAN and LAN. It can be accessed from any computer device in the LAN. For that purpose, at first the assigned IP address has to be checked with the command “ipconfig /all” for Windows OS. The results received are:

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix:
localdomain
```

```
Description: Intel(R) Ethernet
Connection (3) 1218-LM
Physical Address: 68-F7-28-93-89-39
DHCP Enabled: Yes
Autoconfiguration Enabled: Yes
Link-local IPv6 Address:
fe80::9f9e:21e6:flcf:2f7c%10(Preferr
ed)
IPv4 Address:192.168.4.51(Preferred)
Subnet Mask: 255.255.255.0
Lease Obtained: 26 April 2026
10:18:05
Lease Expires: 26 April 2026
11:18:05
Default Gateway: 192.168.4.1
DHCP Server: 192.168.4.1
DHCPv6 IAID: 124319528
DHCPv6 Client DUID: 00-01-00-01-2E-
F0-C1-68-68-F7-28-93-89-39
DNS Servers: 192.168.4.1
4.2.2.2
NetBIOS over Tcpiip: Enabled
```

The GUI of the Raspberry Pi device can be found typing the address 192.168.4.1:444 on any web browser software as the IPFire is using port 444.

The first step in the configuration process should be to activate the Intrusion Prevention Service (IPS) adding provider, which can be found on the Firewall menu (fig. 2).

The Snort/VRT GPLv2 Community Rules is selected as it is proven to be very effective and free. There are available some of the most popular free and not free IPS providers. The firewall has an option to visit the provider website, as well as to enable automatic updates, which in this case is chosen.

From the optional functionalities included IPsec and WireGuard as well as the RED and GREEN interface are activated. Report sending option is also available for configuration (fig. 3). After saving the selectin The IPS is automatically started.

Representing full-scale firewall functionality, the configuration of the IPFire on the Raspberry Pi 4.0 is supported Zone Configuration (fig. 4), Firewall rules (fig.5) and even Location Block services (fig.6) for blocking the traffic from one or more countries.

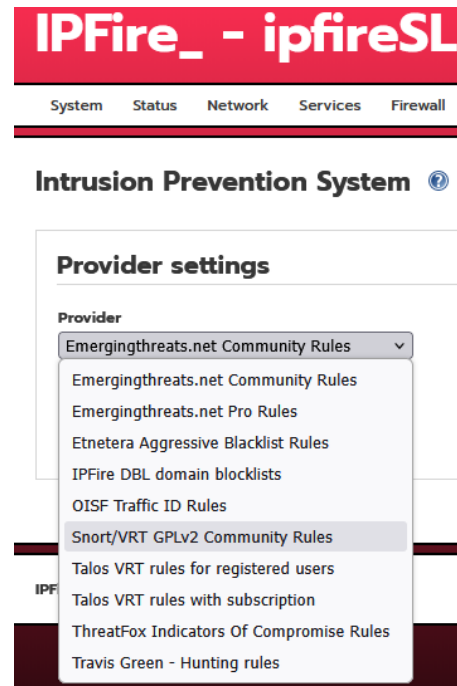


Fig. 2. Provider selection for the IPS.

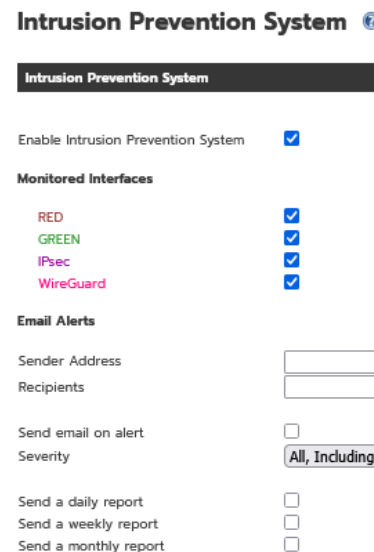


Fig. 3. Selection of the optional functionalities for the IPS.

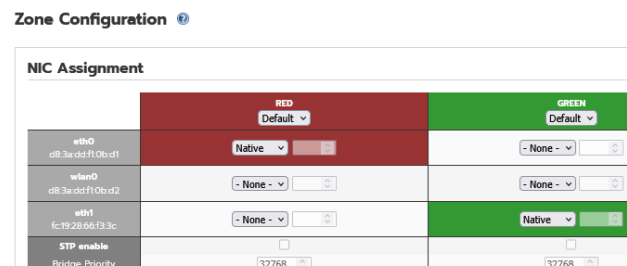


Fig. 4. Zone Configuration for the IPS.

Firewall Rules

Source

☒ Source address (MAC/IP address or network):

☐ Standard networks: Any

☐ Location: A1 - Anonymous Proxy

NAT

☐ Use Network Address Translation (NAT)

Destination

☒ Destination address (IP address or network):

☐ Standard networks: Any

☐ Location: A1 - Anonymous Proxy

Protocol

All

Fig. 5. Adding new rule for the IPS

Location Configuration

Location Block

☐ Enable Location based blocking:

Block countries

Flag	Code	Country
☐	A1	Anonymous Proxy
☐	A3	Worldwide Anycast Instance
☐	AE	United Arab Emirates
☐	AG	Antigua and Barbuda
☐	AL	Albania

Fig. 6. Location Block Configuration.

The location log supported can be analyzed with the firewall log graph (IP) option provided. This is shown on fig. 7.

Firewall-Diagram (IP)

Total number of firewall hits for April 26: 706

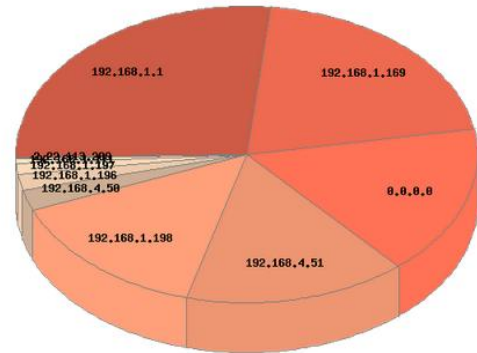


Fig. 7. Firewall log graph (IP).

The Pakfire configuration is used for the installation of some that proved to be very common firewall tools like FreeRADIUS for radius authentication (fig. 8).

Pakfire Configuration

Install

Packages to install: **freeradius**

Checking dependencies..

Package dependencies:

```

Package: freeradius
freeradius -> libtalloc
freeradius -> samba
freeradius -> samba -> avahi
freeradius -> samba -> avahi -> dbus
freeradius -> samba -> avahi -> libdaemon
freeradius -> samba -> libtalloc
freeradius -> samba -> perl-Parse-Yapp
freeradius -> samba -> wsdd
    
```

Packages to install:

```

avahi
dbus
freeradius
libdaemon
libtalloc
perl-Parse-Yapp
samba
wsdd
    
```

Fig. 8. FreeRADIUS installation on Pakfire Configuration.

Another available tool for capturing packets from network traffic is Tshark. One deeper analysis on the lower level is proven to be very useful if the LAN computers are targeted from outside or some unusual traffic is noticed.

III. RESULTS AND DISCUSSION

After an hour of surfing with the firewall on, the operating temperature of the Raspberry Pi 4.0 is not at its peak. The Internet connection speed test shows that it is within the realistically expected norms ~ 85 Mbps. LAN security for a small office or home is proven to be provided

by a pocket Raspberry Pi 4.0, which can be powered by a battery for a long time due to its low power consumption.

For status information analysis, CPU performance (shown in Fig. 9) and average load (Fig. 10) can be visualized graphically on a daily, weekly, monthly, and yearly basis. The memory usage graph is visualized with maximum, average, minimum, and current captions for used, buffered, cached, and free memory displayed (fig. 11).

Status information

Processors

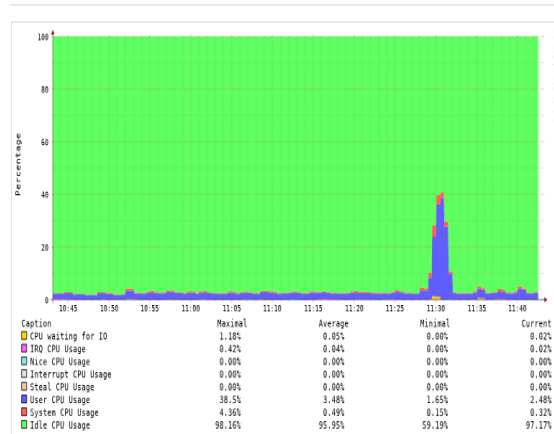


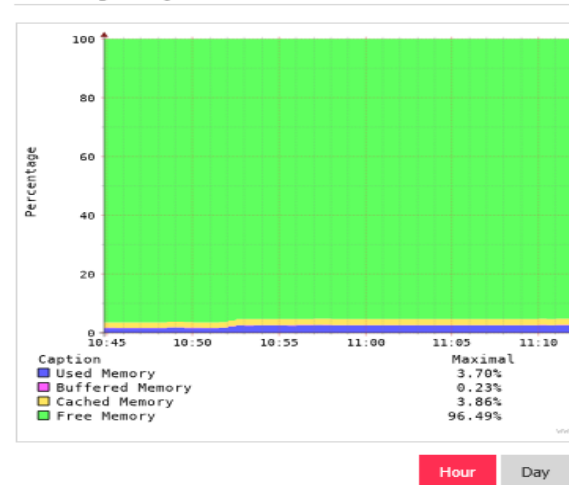
Fig. 9. Status information for the processors' work

Load Average



Fig. 10. Average load status information

Memory Graph



Memory

	Size	Used
RAM	8038216 KiB	415340 KiB
Swap	0 KiB	0 KiB
shared	23816 KiB	
buffers	18664 KiB	
cached	327824 KiB	
available	7622876 KiB	

Fig. 11. Status information for the memory usage of the firewall system

IV. CONCLUSIONS

This approach offers the opportunity to build and maintain basic firewall functionality for computer systems, which can be successfully quickly installed and configured as a backup solution when the main firewall fails. Even not only as a real firewall, IPfire can be successfully used as a monitoring station to monitor for anomalies in daily business traffic. This is also one of the most successfully applied strategies of system attackers. Nowadays, detection and prevention of all types of threats from just one system is often an ability achievable with large investments.

ACKNOWLEDGMENTS

This work was supported by the National Science Program "Security and Defence", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] L. Nikolov, I. Zheleva, D. Mitich, "Network traffic in an intense artillery battery operation", Proceedings of International Scientific Conference "Defense Technologies", 2024, Shumen, National Military University "Vasil Levski", Faculty "Artillery, Air Defense and CIS", pp 372-378, ISSN 2815-4282
- [2] C. Dow, Internet of Things Programming Projects: Build exciting IoT projects using Raspberry Pi 5, Raspberry Pi Pico, and Python, Packet Publishing, 2024., el. ISBN:9781835088685

- [3] D. D. Guinard; V. M. Trifa, *Building the Web of Things: With examples in Node.js and Raspberry Pi*, Manning, 2016. Electronic ISBN:9781617292682
- [4] S. Budiyanto, L. M. Silalahi, A. R. Hakim, A. Hamid, D. Hanafi, "Vulnerability Analysis on Internet of Things (IoT) Networks using Raspberry Pi and Open Web Application Security Project (OWASP)," 2024 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE), Badung, Indonesia, 2024, pp. 58-63, <https://doi.org/10.1109/FORTEI-ICEE64706.2024.10824490>
- [5] H. R. H. Hamid, M. A. I. b. M. A. Kamil and N. Y. Abdullah, "Portable Toolkit for Penetration Testing and Firewall Configuration", 2015, Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 2015, pp. 90-94, <https://doi.org/10.1109/CyberSec.2015.26>
- [6] N. Kurniawati, A. Affandi, I. Pratomo and K. Gyoda, "Raspberry Pi-Based VoIP System For Rural Area," 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia, 2018, pp. 33-38, <https://doi.org/10.1109/ISITIA.2018.8711237>
- [7] N. S. Ismail, N. A. Rashid, N. A. Zakaria, Z. I. Khan and A. R. Mahmud, "Low Cost Extended Wireless Network Using Raspberry Pi 3B+," 2020 IEEE Symposium on Industrial Electronics & Applications (ISIEA), Malaysia, 2020, pp. 1-4, <https://doi.org/10.1109/ISIEA49364.2020.9188215>
- [8] T. Oda, M. Yamada, R. Obukata, L. Barolli, I. Woungang and M. Takizawa, "Experimental Results of a Raspberry Pi Based Wireless Mesh Network Testbed Considering TCP and LoS Scenario", 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Fukuoka, Japan, 2016, pp. 175-179, <https://doi.org/10.1109/CISIS.2016.86>.
- [9] M. C. Xenya, C. Kwayie and K. Quist-Aphesti, "Intruder Detection with Alert Using Cloud Based Convolutional Neural Network and Raspberry Pi," 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA), Cape Coast, Ghana, 2019, pp. 46-464, <https://doi.org/10.1109/ICCMA.2019.00015>.

Turbo Encoders with Hybrid Concatenated Convolutional Design and Turbo Decoders with Soft Input–Soft Output Design in Unmanned Aerial Systems

Georgi Stanchev
Aviation Faculty
Bulgarian Air Force Academy
Dolna Mitropolia, Bulgaria
gstanchev@af-acad.bg

Abstract— Nowadays, unmanned aerial systems play a very important role in the economy, environmental protection, research, and military operations. This is accompanied by constantly increasing requirements for the quality and accuracy of the information received and the commands issued. The elements of these systems operate and perform their tasks by transmitting data and commands over communication radio channels that often face harsh conditions and limitations on frequency-time and energy resources. The conditions for data transfer and command transmission in unmanned aerial systems using channels via communication satellites are particularly difficult. In such channels, the occurrence of single and especially packet errors is a phenomenon with a high degree of probability. The examination and evaluation of the potential capabilities of special class of turbo encoders – with hybrid concatenated convolutional design, to fight against the severe conditions in communication channels in unmanned aerial systems is the main purpose of this research work. Possibilities for optimizing energy consumption and processing time of data flows on board unmanned aerial vehicles through dynamic parameter control of the corresponding turbo decoders with soft input-soft output design are also discussed. Finally, conclusions, recommendations and directions for further research and the application of turbo encoders with hybrid concatenated convolutional design and turbo decoders with soft input and soft output in unmanned aerial systems are made.

Keywords— *communication channel, SISO decoder, turbo encoder design, unmanned aerial system.*

I. INTRODUCTION

Communication technologies used as transfer means of data and control commands between main elements of unmanned aerial systems (UAS) – unmanned aerial

vehicles (UAV), widely known as drones and the command center (CC) – are critical for effective and safe operation of these systems. Autonomous radio channels; Wi-Fi (IEEE 802.11 family) networks; mobile cellular networks (3G, 4G and 5G) and satellite communication networks are commonly used of them, each of which possess certain advantages and disadvantages. Encoding methods and techniques of data and the control commands strongly depend on conditions in these communication media.

In the satellite communication radio channels data and the control commands are highly susceptible to noise, interference and distortions, which lead to significant amount of single and packet errors in the transmitted information.

Strong methods for coding and decoding to correct errors are required to ensure the reliability and efficiency of the tasks and missions of UAS. An encryption in communications channels of UAS to prevent data and control commands from unauthorized access is necessary, as well.

II. MATERIALS AND METHODS

A combination of quantitative and qualitative analysis methods, stochastic methods from Probability Theory, mathematical modelling and computer simulation were used to explore the conditions in the radio channels of UAS, to evaluate the applicability of various turbo codes, as well as approaches for decoding signals damaged by channel noise, in order to correct errors in these channels.

Typical block diagrams of turbo encoders with different internal designs and iterative decoders with soft input and soft output are used to arrive at hypotheses for possibilities

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.30>

© 2026 Georgi Stanchev. Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

for optimizing the use of energy and hardware resources of the equipment, especially that mounted on board the UAV.

A. Satellite Communication Channels

The considerable challenges in ensuring reliable and sustainable operation are reflected in technological complexity, observed in UAVs using cellular and especially satellite communication networks, as shown in Fig. 1.

Satellite communications provide global coverage and are suitable for missions where UAVs operate in remote or hard-to-reach areas – forests, deserts or mountains, and areas without other communication network infrastructure.

However, satellite communication channels suffer from varied and large attenuations due to their large and highly variable physical length. In addition to this, molecular absorption in the Earth's atmosphere, caused primarily by water vapour and oxygen, mismatch between the polarizations of the transmitting and receiving antennas, as well as the inability to use highly directional antennas on board UAVs due to the manoeuvres they perform, lead to an extremely difficult situation regarding to the signal-to-noise ratio (SNR).

For constellations of communication satellites (CS) positioned in low Earth orbit (LEO) the physical length of the channel ranges from 400 to about 2000 km. For highly elliptical orbits (HEO), it can reach up to 42000 km and this is the same order of the communication channel length via a communication satellite located in geostationary orbit (GEO), when it is visible at low elevation angles.

This attenuation, caused by the distance D between the transmitter and receiver in the communication line can be estimated by the expression (1):

$$L_0 = 20(1.1 + lgD - lg\lambda), dB \quad (1)$$

where λ is the wavelength of radio signals.

The molecular absorption of radio signal energy in the Earth's atmosphere is mainly due to oxygen and water dissolved in it, and can be accounted for by expression (2).

$$L_a = \frac{[L_{O_2}(h_{O_2} - h_s) + L_{H_2O}(h_{H_2O} - h_s)]}{\sin\theta}, dB \quad (2)$$

where L_{O_2} [dB/m] is the specific absorption coefficient and h_{O_2} [m] is equivalent atmospheric height for oxygen, L_{H_2O} and h_{H_2O} are the same ones for water dissolved in the air, h_s is the altitude of the UAV, communicating with satellite, and θ is the elevation angle of the communication satellite above the horizon.

Other factors leading to signal attenuation in the long satellite communication links include absorption by hydrometeors, dust and smoke in the lower layers of the atmosphere, as well as obstruction by tall vegetation, buildings and others.

The accurate assessment of these additional losses (L_d) is a complex problem of a stochastic nature, in the solution of which the climate model of Crane is often used [1].

The total signal power losses L_z are defined as (3):

$$L_z = L_0 + L_a + L_d, dB \quad (3)$$

Therefore, it is very difficult to predict accurately the total attenuation in satellite communication channels, which is why some redundancy in terms of signal power is mandatory.

Another aggravating circumstance is that antennas with high gain, i.e. with sharp directivity diagrams, are not used on board UAVs to ensure their manoeuvrability. This gives a result in an even worse SNR compared to the lines between a communications satellite and a fixed earth station. At the same time, it remains pointless to take into account the losses from tropospheric and ionospheric refraction of radio waves, which are different in cause but the same in result as the losses coming from inaccurate pointing of antennas towards each other in the radio channels between receiver and transmitter if at least one of whose antennas is non-directional.

In the satellite communication channels is observed Doppler shift F_D and signal spectrum broadening with significant values and fluctuations, especially at CS on LEO. The large Doppler shift of the frequency spectrum of the signals means that the receiver bandwidth must be expanded to capture them. Expanding the frequency band of the receiver beyond the width of the frequency spectrum of the signals means a deterioration of the SNR. Therefore, the lower attenuation of signals in LEO-based systems compared to those using GEO is to some extent compromised by the high noise level after the receiver input and the associated low SNR.

The Doppler shift of the signals in this case can be represented as a function of the altitude H_s and the inclination i of the orbit of the CS, the latitude B of the UAV and the time t , i.e. $F_D(H_s, i, B, t)$. [2]. The Doppler shift in one communication system is a result of the radial velocity $V_R(t)$ between the transmitter and the receiver communicating:

$$F_D = -F_0 V_R(t) [V_R(t) + c]^{-1}, Hz \quad (4)$$

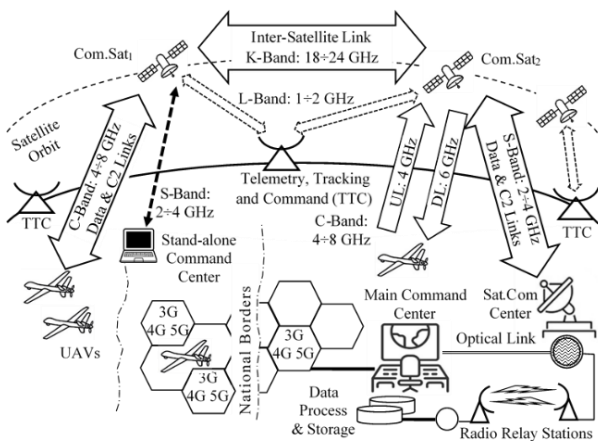


Fig. 1. UAS on cellular and satellite communication networks.

where $c = 2,998.10^8$ m/s is speed of light.

The change in the distance $D(H_s, i, B, t)$ between CC or UAV and CS determines the radial velocity V_R between them:

$$V_R(H, i, B, t) = \frac{\partial D(H, i, B, t)}{\partial t}, m/s \quad (5)$$

and the solution of the task of determining the Doppler shift F_D is reduced to deriving an expression for the instantaneous distance between CC or UAV and CS.

Although the variation is complex and the amplitudes are large, the Doppler shift is accurately predictable, e.g. Doppler shift in Globalstar satellite communication system – Table 1, especially if the latitude of the CC or UAV, the 22 km difference between the equatorial and polar radii of the Earth, and the ephemeris data of communication satellites are taken into account [3]. Thus, it is possible to compensate for the Doppler shift of the signals if the UAV is equipped with a receiver of a global positioning system. Then by an appropriate control of the heterodyne frequency in the super-heterodyne receiver, the intermediate frequency can be stabilized, despite the Doppler shift.

TABLE 1. DOPPLER SHIFT IN GLOBALSTAR SATCOM SYSTEM.

$H_s=1414$ km (LEO), $i=52^\circ$; $f_0=2,5$ GHz (Down Link XIII ch.) Absolute Doppler shift, kHz			
Maximum elevation, θ_{max}	30°	60°	90°
Latitude of UAV $B=42^\circ$ N	$\pm 37,75$	$\pm 44,75$	$\pm 45,75$
Latitude of UAV $B=0^\circ$ (equatorial position)	$\pm 37,25$	$\pm 44,63$	$\pm 45,75$

In addition to the large and highly variable attenuations and Doppler shifts, the control and data transfer between CC and UAVs in UASs using communication satellites is characterized by significant latency due to the large distances that signals must overcome in such systems. Signal processing (encoding and decoding) with powerful error correction codes in systems with communication channels suffering from low level of SNR leads to an additional increase in this latency. As a result, control commands arrive at the UAVs with a noticeable delay.

However, UAVs are extremely fast and highly maneuverable flying vehicles due to the absence on board of a human. If, during a complex task, the UAV needs to abruptly change its flight mode and the command for this is not recognized correctly, then retransmission of commands or automatic repeat request (ARQ) mode are not suitable precisely because of this latency.

The aforementioned characteristics of satellite communication networks as a medium in UAS are a prerequisite for special attention to the reliability and error protection of data and commands transmitted in these systems. To increase the reliability of transmitted control commands and data transfer in unmanned aerial systems, the implementation of channel coding with error correction codes is absolutely necessary [4]. The accurate choice of Forward Error Correction (FEC) code depends on both the

specific requirements of the communication system and the characteristics of the communication channel [5], [6].

Fig. 1 shows the communication channels used to connect between the elements of a complex UAS, passing through communication satellites. The appropriate frequency ranges are indicated, and the principle of comparability of the powers of the receiver inputs is observed in the distribution of the frequency bands between up-link and down-link. This means that when the energy resources of the various elements of the communication system are unequal, and therefore the radiated power capabilities, the higher frequency part of the range is assigned to the element with the greater energy capabilities. The greater attenuation from molecular absorption in these higher frequency bands equalizes the power levels at the receiving points. Elements of the separate Telemetry, Tracking and Command (TTC) system are also shown.

B. Turbo Encoders in UAS– Features and Design

There are several types of error correction codes suitable for use in the harsh conditions in communication channels of UAS using satellite communication networks [7]. Such are Low Density Parity Check (LDPC) codes; Reed-Solomon codes, which are a special case of Bose–Chaudhuri–Hocquenghem (BCH) codes; non-separable continuous codes with a subsequent interleaving process, often in combination with some of the block codes mentioned above, applied as outer ones.

Turbo codes are particularly suitable for application in any kind of systems using satellite communication channels. This relatively young class of FEC codes, which are the first practically usable ones bringing the actual channel capacity very close to its maximum (Shannon limit), have convincingly proven their effectiveness and have found application in 3G (UMTS) and 4G (LTE, IEEE 802.16 – WiMAX) mobile cellular communications, in satellite communications and deep space communications.

The most valuable characteristics of turbo codes are superior error correction performance, enhanced decoding accuracy, robustness in noisy environments, efficiency at low SNR , adaptability for different applications, reduced bandwidth requirements, handling burst errors and energy efficiency [8], [9]. These useful properties of turbo codes are achieved at the expense of some certain disadvantages compared to traditional FEC codes. Most of these drawbacks are due to the requirements of the turbo code decoding process. The more significant of them are computational complexity, demands for larger volumes of memory, more energy consumed and more latency at the decoding process, especially when implementing iterations. Other common drawbacks of error protection using turbo codes are the sensitivity to the design of the interleaver (Π block) in combating packet errors and lack of universal suitability, because turbo codes are not optimal for short data blocks.

The classic design of turbo encoder, shown in Fig. 2 [10], explains the main idea that allow achieving the unique characteristics of turbo codes.

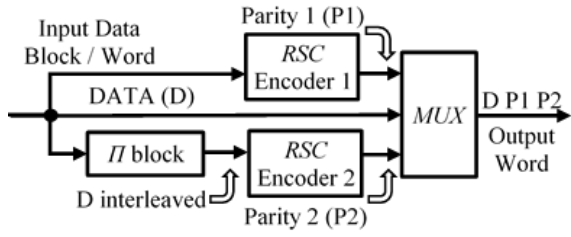


Fig. 2. Classic design of turbo encoder.

Two parity sequences, achieved by working on different arrangements of the same block of data, together with the original data block are sent through noisy channel. The inner encoders in that design, used to obtain parity sequences are recursive systematic convolutional (RSC) encoders, which differ from non-recursive ones due to the presence of feedback in their shift-register pattern, making them filters with an infinite impulse response [11], [12].

One RSC encoder with constraint length K of 4 in form of a chain of memory cells and a feedback, realized by shift-registers (D-Triggers) and Boolean XOR function units is shown as an example in Fig. 3. The feedforward polynomial $G(D)$, describing the parity output, is:

$$G(D) = D + D^3 \quad (6)$$

and the polynomial $F(D)$, describing the feedback, is:

$$F(D) = 1 + D^2 + D^3 \quad (7)$$

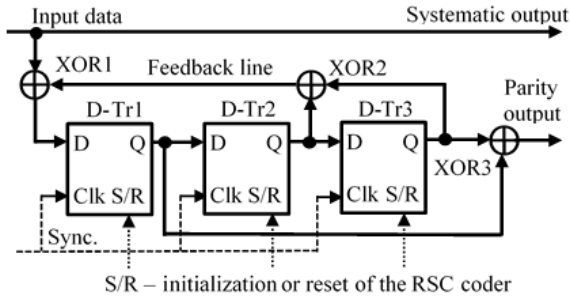


Fig. 3. An example of RSC encoder design.

Based on this classic turbo encoder design, several basic types have been developed and used. They differ in the type of specific encoders embedded in the basic circuit, additional devices such as interleaving blocks and memory blocks, as well as the way in which these essential elements are connected in the overall turbo encoder circuit. These particularities in the design naturally lead to different properties of the resulting turbo codes, such as capabilities for combating different types of errors, applicability to different types of data and conditions in the communication channel, latency, capabilities for adapting to different speeds and volumes of the processed data blocks, computational complexity, power consumption, etc. [7].

a) Parallel-concatenated convolutional (PCC) encoder in which certain number of RSC encoders are producing different parity blocks by working in parallel on variants of one and the same data block. Encoder with PCC design is shown as an example in Fig. 4.

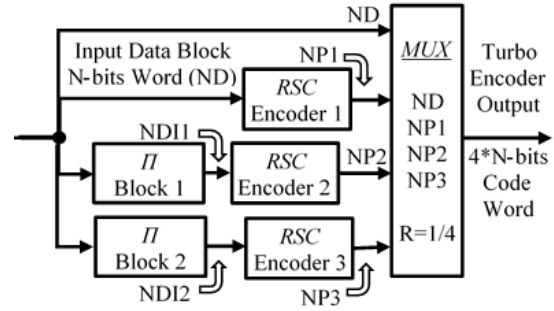


Fig. 4. An example of turbo encoder with PCC design.

The required number of interleavers provides the different variants of the data block. A structure of PCC turbo encoder consists of three RSC encoders and two interleavers. This turbo encoding has high coding gain and is appropriate to UASs where reliability and low latency are strongly required, e.g. satellite communication lines.

b) Serial concatenated convolutional (SCC) encoder – it uses convolutional encoders in a serial configuration, so the data stream at the output of one of the decoders is input data stream to the next one. This type of codes are very suitable for iterative decoding, which is the essential point when transferring data using turbo codes. The typical SCC encoder includes outer convolutional coder, which processes input from a data source, an inner convolutional encoder that transmits its output data stream to a noisy channel, and an interleaver that connects the two encoders, as illustrated in Fig. 5.

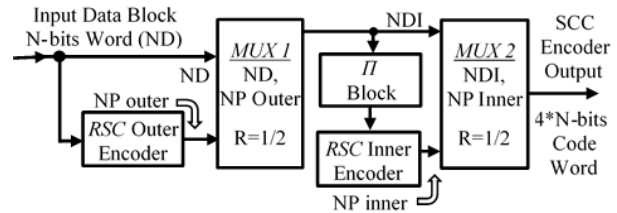


Fig. 5. An example of turbo encoder with SCC design.

Because inclusion of an RSC encoder as an inner encoder, turbo codes generated by encoders with SCC design have better characteristics compared to codes generated by encoders with PCC design around error floor – the area after which the trend of decreasing of the bit error ratio (BER) with increasing SNR decreases significantly.

c) Hybrid concatenated convolutional (HCC) encoder, which combines both serial and parallel connections between its built-in RSC encoders, and the relevant interleavers included in the structure – Fig. 6.

The combining of the two main types of connection between the built-in RSC encoders allows the turbo encoders with the HCC design to inherit from PCC encoders the high coding gain at low SNR and from the SCC the low error floor at high SNR [13]. Furthermore, the complex HCC design allows an adapting the encoder to different coding rates, by puncturing (taking away part of the parity bits according to a certain pattern) at several points in the connection scheme.

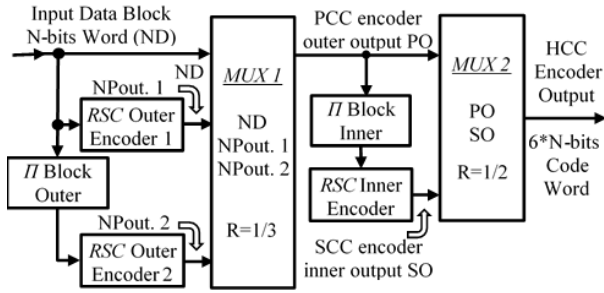


Fig. 6. An example of turbo encoder with HCC design.

It should be borne in mind that during the execution of a mission, the distance between the *CC* and the *UAV*, and thus the *SNR*, varies widely. These changes are even more drastic if a satellite communication network with satellites on *LEO*, is used as the medium between the *UAS* elements. Turbo codes with *HCC* design, with their ability to adapt to different data types, coding rates and data rates, as well as to work well under different conditions in communication channels, copes with these challenges to a high degree.

The superior performance of codes generated by turbo encoders with *HCC* design over a wide range of *SNR*, as well as the ability to work with different data types makes them extremely suitable for *UAS*.

C. Iterative Turbo Decoding

The design of the decoders in the receiving devices is intrinsically linked to that of the encoders in transmitting devices, with variations in decision-making methods for received code words. Although algorithms based on hard decisions (according to Hamming distance between code words) are significantly easier and more economical to implement, nowadays those based on soft decisions (according to Euclidean distance), iterations and inner information exchange are mainly used.

In radio communication channels, in the presence of Additive White Gaussian Noise (*AWGN*), opposing signals, as Binary Phase Shift Keying (*BPSK*) modulated ones, are best distinguished. In these cases computer data u_k (0 or 1) are mapped as opposite channel symbols x_k (1 or -1) by the rule:

$$x_k = 1 - 2u_k \quad (8)$$

In this case, the *XOR* (*exclusive OR*) operation, often used in computer science, is completely adequately replaced by the "multiplication" operation used in communication technology.

The typical turbo decoder with soft-in soft-out (*SISO*) design is based on the assumption of an independent input sequence and a memoryless channel and its structure and the nature of the processes within it explains some of the shortcomings of turbo codes listed above.

In turbo decoders with built-in *SISO* decoders, soft decisions are presented and processed by Log-Likelihood Ratio (*LLR*), of the evaluated signals. As an example when the received *BPSK* signals are evaluated in channel decoder, the ratio of the conditional probabilities for the transmission of x_k or $-x_k$ is used, given a received signal y_k :

$$LLR = \ln \left[\frac{P(x_k/y_k)}{P(-x_k/y_k)} \right] \quad (9)$$

The aim is to obtain large values of $|LLR|$, which means great certainty in making a decision, and the sign in front of the *LLR* indicates which of the two signals (x_k or $-x_k$) is more likely. *LLR* values close to zero indicate serious uncertainty in the decisions and at $LLR=0$ there is complete uncertainty. The value of $|LLR|=3$ corresponds to 95.5% confidence in the estimate for one or the other symbol. The natural logarithm is chosen for convenience in determining the estimate of symbols passed through a communication channel with *AWGN*, since the nature of this noise assumes a Gaussian (normal) probability distribution of amplitudes.

Other relationships that are valid in this way for probabilistic symbol evaluation are:

$$P(x_k) = (1 + e^{-LLR})^{-1}; \quad P(-x_k) = 1 - P(x_k) \quad (10)$$

If there is only one decoder, it must make a hard and final decision about the meaning of the received symbol. Two or more decoders can participate in a soft decoding scheme, in which the decoders exchange soft information - an estimate of the meaning of a received symbol, with some degree of confidence in that estimate. *LLR* is precisely the format in which these soft-input soft-output decoders exchange such soft information. Turbo coding shows its superior qualities best if, when evaluating a single symbol, the process of exchanging soft information between *SISO* decoders is repeated many times before a final hard decision is made – so called *iterative decoding*.

The *SISO* decoders built into the turbo decoders implement the Bahl-Cocke-Jelinek-Raviv (*BCJR*) algorithm, which is particularly suitable for decoding convolutional codes and provides maximum a posteriori (*MAP*) estimate for defined trellis, i.e. turbo codes with a specific structure, determined by the block diagram and parameters of the turbo encoder. To achieve this, the *BCJR* algorithm calculates and combines three types of metrics (probabilities): forward metric α_{k-1} , backward metric β_{k-1} and branch metric (probability of transition) γ_{k-1} .

Generally speaking, a posteriori information LLR_{post} has the following structure:

$$LLR_{post} = LLR_s + LLR_{apr} + LLR_{ext} \quad (11)$$

where LLR_s is the evaluation of the systematic symbol by the channel decoder, LLR_{apr} is some quantity of a priori information.

Each *SISO* decoder produces extrinsic information LLR_{ext} that is sent and used by the other *SISO* decoder as a priori information LLR_{apr} . The new produced information is extracted using the parity symbols, which also pass through the noisy channel and therefore the estimate for them is in the form of Log-Likelihood Ratio LLR_{par} . This extrinsic information at the output of any *SISO* decoder does not repeat parts of the information at the input of this *SISO* decoder, thus avoiding overconfidence of the overall turbo decoder:

$$LLR_{ext} = LLR_{post} - LLR_s - LLR_{apr} \quad (12)$$

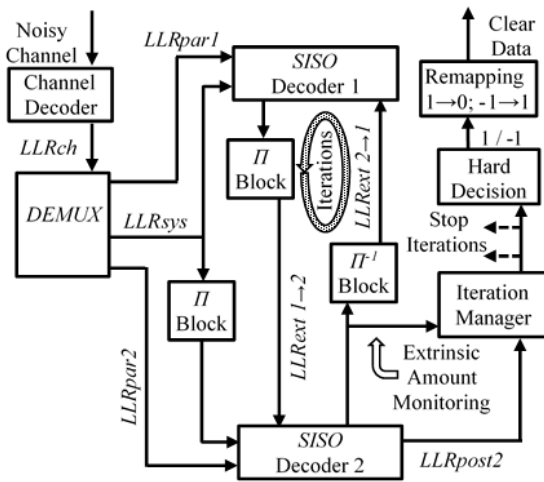


Fig. 7. Turbo decoder with built-in channel and SISO decoders.

A turbo decoder with two embedded SISO decoders iteratively exchanging extrinsic information and controlling the iterations is shown in Fig. 7.

From the internal information exchange algorithm and the sequence of iteration stages, it is clear that each portion of extrinsic information at the output of one SISO decoder is a priori information at the input of the other SISO decoder. The exchange breaks by the iteration manager, which stops the process upon reaching certain criteria.

III. RESULTS AND DISCUSSION

Analysis of the shortcomings of turbo codes shows that they are primarily related to providing more energy resources and hardware complexity and capabilities for decoding processes. Unfortunately, these qualities are lacking in UAV equipment and power supplies.

Given the theoretical and constructive considerations described above, several approaches can be considered for optimal use of the energy and hardware resources of the elements of a UAS using satellite communication channels in its structure. Searching for and finding such solutions is especially important for UAVs, where the limitations of these resources, as well as mass, volume, and aerodynamics and maneuverability requirements, are severe.

One approach to optimizing two-way communications between the UAV, on the one hand, and the ground CC or communication satellite, on the other, is to use asymmetric FEC coding schemes in the opposing channels - Fig. 8

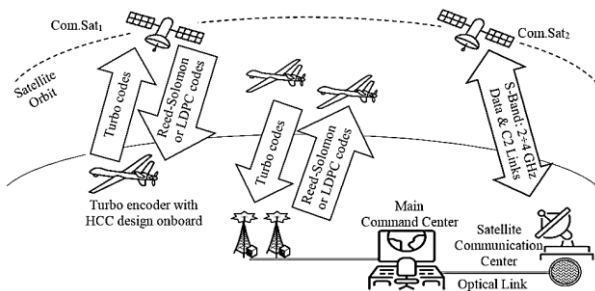


Fig. 8. Asymmetric FEC encoding to and from UAV.

This means that on board the UAV, blocks of data can be encoded against errors with powerful turbo codes, since on the ground (in the command center) or on board the communication satellite, there are more energy and hardware resources to overcome the higher demands of the turbo code decoding processes. In the communication channels to the UAV, the information flow consists primarily of commands, which are essentially short blocks of data, where turbo codes are not particularly effective anyway.

To protect data from errors in the communication channels towards the UAV, it seems appropriate to use LDPC or Reed-Solomon block codes, which outperform turbo codes when dealing with short data blocks. In addition, protection against errors in these channels can be enhanced by providing a higher level of signal-to-noise ratio at the input of the UAV receiving equipment, since the ground CC or communication satellite, having greater energy resources than those of the UAV, can afford higher transmission power.

Analysis of a typical family of *BER* versus *SNR* characteristics (shown in Fig. 9) of performance of iterative turbo decoder at different number of iterations shows some interesting facts that can be used for an optimization [12].

First of all, it is noticeable that a drastic drop in *BER* occurs in the first few iterations. For example, at an *SNR* of around 1.5 dB, the *BER* drop between the first and third iteration is almost three orders of magnitude (1000 times). At the same time, for the same *SNR*, the *BER* drop from the sixth to the eighteenth iteration is insignificant.

Next, it is seen that this disproportionality in the significance of the first and subsequent iterations for *BER* reduction increases with increasing *SNR*. Furthermore, it is evident that the presence of an error floor makes it meaningless to increase the number of iterations above a certain reasonable limit, which remains adequate for a wide range of *SNR*.

Since in satellite communication lines the distance between the communication satellite and the UAV is very variable, and as a result the *SNR* fluctuates within large limits, maintaining a given *BER* level requires a significant reserve of computing power, for the sake of energy resources. In addition to distance, the position of the opposing equipment relative to the antenna's directional pattern also matters. This can be avoided by setting a certain *BER* threshold, which is different for different data types, and then applying a variable number of iterations required to bring the *BER* below this threshold. Thus, the number of iterations, and thus the consumption of energy resources, is set depending on the *SNR* in the channel or the distance between the communication satellite and the UAV, without unnecessary losses.

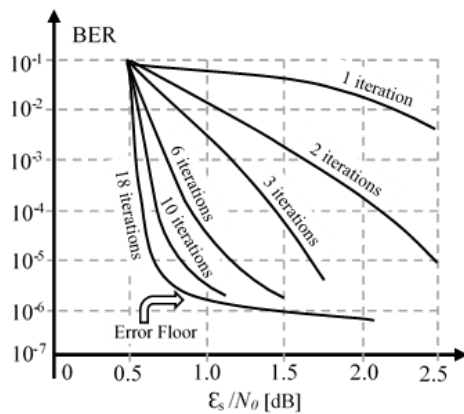


Fig. 9. Typical iteration family of characteristics BER vs. SNR.

Instead of the distance between the communication satellite and the UAV, a more accurate criterion can be the extrinsic information exchanged between the *SISO* decoders during turbo decoding. When the amount of such information falls below a certain level, set by the required *BER*, the iteration manager that monitors it stops the iterations and issues a command to make a hard decision based on the a posteriori information at the output of the second *SISO* decoder, reached up to that point.

IV. CONCLUSIONS

The conditions in the communication channels for data and control commands transfer in UAS are extremely difficult, especially if communication satellites are used.

Therefore, a few key points need to be considered:

- Different types of digital data in communication channels have different sensitivity to errors occurring during their transmission. Command and control signals, even at the lowest data rate, should be maximally protected from errors and at the same time, this should be done through encoders and decoders that introduce minimal additional latency. Turbo codes are not optimal for short blocks, where LDPC and BCH codes are more effective. The possible solution is in asymmetric encoding – the FEC codes used in the direction from CC or communication satellite to UAV and in the opposite direction are of different types and characteristics.

- Turbo codes have superior performance at low *SNR*. However, they require more power and hardware resources, especially during decoding. In the channels to the UAV, a higher *SNR* can be achieved at the expense of the capabilities of the ground and satellite equipment to transmit signals with higher power, i.e. this is another argument for using asymmetric FEC coding. In addition, ground and satellite stations can afford to use directional antennas in the channels to UAVs, which further improves the *SNR* at the inputs of the receiving equipment.

- Turbo encoders with *HCC* design cover a wide range of requirements and characteristics of the satellite communication channels. In addition, they contain in their complex structure all the necessary blocks and connections

to switch on command and as needed, thereby becoming encoders with *PCC* or *SCC* design. This makes them applicable to UAS, which use satellite communication networks for control and data transfer to and from UAVs.

- Optimization of the use of energy and hardware resources can also be achieved through the development and research of more complex and intelligent algorithms for managing iterations and other processes in turbo code decoders. This would lead to opportunities for energy and hardware, with their attendant mass and volume, to be allocated to improving other mission characteristics and the effectiveness of UAS in general.

ACKNOWLEDGMENTS

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

- [1] R. K. Crane, A Two-Component Rain Model for the Prediction of Attenuation and Diversity Improvement. New Hampshire Hanover: Dartmouth College, 1982.
- [2] G. Stanchev, "Research on the robustness of a digital satellite communication system using noise-like signals" (in Bulgarian), PhD thesis, Rakovski National Defence College, SNS "ASUIVO", Sofia, Bulgaria, 2001.
- [3] G. Stanchev, Satellite Communications (in Bulgarian), Veliko Tarnovo: National Military University "Vasil Levski", 2006, pp. 38-39, ISBN-10:954-713-078-1, ISBN-13:978-954-713-078-4.
- [4] T. S. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall; Subsequent edition, 2002, pp. 339-356.
- [5] S. Lin and D. J. Costello Jr., Error Control Coding, London: Pearson, 2nd edition, 2004, pp. 257-315.
- [6] B. Sklar, Digital Communications: Fundamentals and Applications. (Скляр, Б., Цифровая связь – теоретические основы и практическое применение. Второе издание, исправленное. М., "Вильямс", 2004.) pp. 332-452.
- [7] G. Stanchev and V. Katsarska, Application of Turbo Codes in Unmanned Aerial Systems, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 16th International Scientific and Practical Conference, June 19th–20th, 2025, Volume II, pp. 329-336, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2025vol2.8575>
- [8] K. Sripimanwat, Turbo Code Applications (a journey from a paper to realization), New York: Springer, 2005.
- [9] B. Vucetic and J. Yuan, Turbo Codes: Principles and Applications, New York: Springer Science+Business Media LLC, 2000, pp. 73-80. ISBN 978-1-4613-7013-0.
- [10] C. Berrou and A. Glavieux, Near Optimum Error Correcting Coding and Decoding: Turbo-Codes, IEEE Trans. on Communications, vol.44, No.10, October 1996, pp. 1261-1271.
- [11] J. G. Proakis and M. Salehi, Communication System Engineering, 2nd edition, PHI Learning Private Limited, New Delhi, 2011, pp. 591-601.
- [12] J. G. Proakis and M. Salehi, Communication System Engineering, 2nd edition, PHI Learning Private Limited, New Delhi, 2011, pp. 640-646.
- [13] D. Mishra, S. Jit and K. Dasgupta, Hybrid Concatenated Convolutional Code for Deep Space Mission, International Journal of Computer Applications (0975 – 888), Volume 47– No.19, June 2012, pp. 33-38.

Public Trust as a Bridge between Technology, Society, and Sustainability

Dimitrina Stefanova

Department "Public Relations"
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria

d.stefanova.swu@gmail.com

Kristiana Bacheva

Department of Library Science
University of Library Studies and
Information Technologies, Sofia,
Bulgaria

christiana.stefanova05@gmail.com

Valentin Vasilev

New Bulgarian University
Sofia, Bulgaria
v.vasilev@nbu.bg

Abstract— The accelerating processes of digital and energy transformation are fundamentally reshaping contemporary societies, economies, and governance systems. While technological innovation and the transition to sustainable energy are essential for long-term development, their success increasingly depends on the level of public trust. In this context, trust emerges as a critical factor and a central mechanism linking technological advancement with societal acceptance and sustainability outcomes.

Growing concerns related to data privacy, algorithmic opacity, misinformation, and perceived inequalities in energy access challenge public trust and, consequently, the legitimacy of institutional and corporate actors, as well as broader systems of governance and security. The discussion is positioned within an interdisciplinary framework that integrates perspectives from technological sciences, communication studies, and sustainability governance. The present study aims to examine the key components of public trust, as well as the factors generating uncertainty in the context of technological transformation.

The author's contribution lies in advancing the existing scholarly debate on the social dimensions of technological transformation by offering practical insights for experts and organizations seeking to align innovation with societal expectations through trust-based approaches.

Keywords: trust; digital transformation; strategic communication; ethical governance; sustainability.

I. INTRODUCTION

Public trust in technology is multifaceted and wide-ranging, involving diverse analytical perspectives and research approaches. Technological transformation in the modern digital age is generating profound and multidimensional changes across all spheres of social life. The Industry 5.0 paradigm, based on the interaction between people and technology, creates new opportunities for innovation, efficiency, and sustainable development, while simultaneously posing significant challenges related to trust in technology, the organizations that develop and

manage it, and the institutions responsible for regulatory oversight.

The lack of a global consensus on technology governance, ethical standards, and regulatory frameworks reinforces perceptions of uncertainty and mistrust among social groups. Risks such as data breaches, algorithmic opacity, the cumulative effects of technology scandals, disinformation, and expanding digital surveillance practices undermine trust and call into question the legitimacy of technological progress. Systemic manifestations of distrust are further exacerbated by risks associated with artificial intelligence, growing digital inequality, and the migration of a significant portion of social interaction to virtual environments. These processes create conditions for social isolation, online harassment, and various forms of digital coercion, while simultaneously reinforcing asymmetries in access to technology and information.

In the context of growing cyber threats, the so-called zero-trust model has gained prominence [1] [2], transforming traditional security approaches from the "trust but verify" logic to the "never trust, always verify" principle. Furthermore, the accelerated development of automated technologies creates conditions for new, often unpredictable risks that require adequate communication and management responses.

Although positive trends in trust levels can be observed in certain sectors, concerns continue to act as significant barriers to their full public acceptance and support. In this sense, technological innovations, in synergy with dynamic political and social processes, act as a factor with a dual impact: on the one hand, as a driver of development, competitiveness, and sustainability; on the other, as a source of growing public distrust, uncertainty, and skepticism. This necessitates the development of systematic debates and integrative frameworks that combine technological, social, governance, and communication solutions within a human-centered

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.158>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

paradigm. Within this framework, the technology sector, ethical governance, and stakeholder engagement play a key role in promoting both sustainable development and trust.

At the same time, technology serves as a key catalyst for achieving the Sustainable Development Goals, enabling the adoption of green and eco-friendly technologies, the development of renewable energy, the implementation of circular economy principles, and the use of innovative solutions such as artificial intelligence, blockchain, and smart city infrastructures. At first glance, this may seem paradoxical. Nevertheless, it can reasonably be argued that trust serves as a central connecting mechanism between technological development and sustainability.

In this sense, sustainable development requires a balanced approach in which technological solutions are integrated with strategic communication, ethical governance, and active public trust-building as a prerequisite for their effective and inclusive implementation.

II. MATERIALS AND METHODS

The subject of this study is, by its very nature, multifaceted, interdisciplinary, and multidisciplinary.

The methodological tools used in the study include desk research, content analysis, document analysis, comparative analysis, and a deductive approach. The study is based on an interdisciplinary framework that integrates perspectives from communication studies, the management of technological development and implementation, and research in the field of sustainable development. Scientific publications and strategic as well as empirical data from the Edelman Trust Barometer have been analyzed. Additionally, the White Paper on Artificial Intelligence: A European Approach to Excellence and Trust is utilized, which provides a conceptual framework for examining the relationship between technological development and public trust, and more specifically, the potential significant impact of AI on our society and the need to build trust. The aim of the study is to identify key relationships between technological innovation, institutional legitimacy, and sustainable development that influence public trust, in order to more clearly outline the research framework of trust as a bridge between technology, society, and sustainability.

III. RESULTS AND DISCUSSION

This study aims to contribute new insights to the academic debate on the relationship between technological progress and sustainable development. It is based on the understanding that technological progress does not automatically lead to sustainability, but rather requires purposeful management of its social, ethical, and institutional dimensions.

The central thesis is linked to the premise that contemporary technological transformation requires a process of dual adaptation. On the one hand, it should be noted that individuals and organizations must develop technological competencies and the capacity to adapt quickly to innovations. On the other hand, the technologies themselves must be designed and managed in accordance with human values, ethical principles, and societal

expectations. In this sense, technological development cannot be considered sustainable without the integration of a “human face,” i.e., an orientation toward human well-being, dignity, and security. This interdependence between human adaptation and human-centered technological design positions trust as a key mediator and connecting mechanism in the processes of digital and social transformation.

At the same time, it must be clearly recognized that technological progress is inextricably linked to institutional trust, which plays a critical role in mitigating risk and ensuring regulatory protection for citizens. From this perspective, sustainable development requires a balanced interplay between innovation, regulation, and trust, in which technologies are embedded within a framework that guarantees security, transparency, and the protection of the public interest.

Research and Findings: From Empirical Evidence to Theoretical Insights

The 2026 Edelman Trust Barometer reveals a significant shift from broad, institutional trust to a more isolated and localized form of trust. Distrust is increasingly becoming the default, with only one-third of respondents stating that most people can be trusted.

This contraction of trust is accompanied by growing social fragmentation and polarization, reflected in widening trust gaps between income groups and declining trust in institutions. Trust is increasingly concentrated in immediate circles such as employers, CEOs, and personal networks, rather than in governments or global systems. At the same time, economic uncertainty, geopolitical tensions, and the legacy of crises such as COVID-19 have intensified skepticism toward authority and expertise.

The consequences of this transformation are significant. First, there is growing resistance to technological change, particularly regarding artificial intelligence, where a majority in key economies express distrust and concerns about transparency. Second, rising nationalism is evident in the growing preference for local over global actors. Third, societies are showing a reduced capacity for collective action, particularly in areas such as climate policy. Finally, there has been a significant decline in optimism, with only 15% of respondents in developed markets believing that future generations will be better off.

In response to these trends, the report introduces the concept of “trust brokering,” highlighting the role of institutions especially employers—as intermediaries capable of restoring trust. By translating complex global challenges into tangible and locally meaningful actions, these actors can serve as critical links between systemic change and individual experience. [3].

Data from the 2026 Edelman Trust Barometer [4] further shows that trust, traditionally associated with progress, cooperation, and institutional legitimacy, is under increasing pressure and is gradually shrinking to narrower, closer social circles. This trend calls into question the sustainability of social systems that, by their very nature, rely on extended networks of trust rather than limited, closed communities.

In this context, a critical question arises: can we speak of an “implosion of trust” a process in which trust does not disappear entirely, but rather becomes compressed, fragmented, and localized? If trust withdraws from

institutions and concentrates in personal and informal relationships, what are the consequences for governance, innovation, and sustainable development?

From a sustainability perspective, this phenomenon is twofold. On the one hand, localized trust can strengthen internal cohesion within smaller communities and networks. On the other hand, the weakening of institutional trust undermines the capacity for collective action on a broader scale, and this depends on the type of coordinated efforts for example, those needed to address global challenges such as climate change, digital transformation, and social inequalities.

Therefore, the key question is not whether trust is declining, but how it is transforming and how it can be reimagined as a resource for resilience. Is it possible to develop a new model of “distributed trust” that combines local proximity with institutional legitimacy? And what is the role of technology in this process will it deepen fragmentation, or can it serve as a mechanism for restoring trust through transparency, participation, and accountability?

In this sense, sustainability in the digital age requires not only the management of resources and technologies, but also the strategic management of trust as a form of social capital. It is precisely at this intersection that the need arises for new communication and management approaches capable of restoring the connection between institutions, technologies, and society.

The interdependence between trust and sustainability becomes increasingly evident when viewed through the lens of contemporary global trends. Diminishing optimism about the future significantly reduces people’s willingness to support long-term strategies, including investments in clean energy, sustainable mobility, and inclusive social policies. When expectations for the future wane, so does the motivation to participate in collective efforts that require deferred but shared benefits.

The findings of the Edelman Trust Barometer 2026 clearly show that sustainable transformation cannot be achieved without trust. It should not be understood simply as a relational or emotional construct, but as a form of institutional and social infrastructure that enables economic, environmental, and societal transitions.

In the context of declining trust in government, business is increasingly viewed as a stabilizing force in society. It is expected not only to deliver economic value but also to contribute to social cohesion, ethical governance, and constructive public dialogue. Through their policies, partnerships, and tangible actions, organizations have the capacity to mitigate negative externalities and actively drive positive social change.

Public Trust: Theoretical Foundations and Conceptual Perspectives

Public trust is widely recognized as a fundamental element in the functioning of modern societies, especially in contexts characterized by increasing complexity, uncertainty, and rapid technological change. It serves as a critical mechanism that enables cooperation, reduces perceived risks, and supports the legitimacy of institutional and organizational actors.

From a classical sociological perspective, Niklas Luhmann conceptualized trust as a mechanism for reducing social complexity. In situations where individuals cannot fully assess risks or predict outcomes, it allows them to act despite incomplete information [5]. This interpretation positions trust as a cognitive and systemic tool that facilitates decision-making in an uncertain environment.

Similarly, Francis Fukuyama defines it as a form of social capital embedded in shared norms and values that enable cooperation within societies [6]. From this perspective, high-trust societies demonstrate greater capacity for innovation, economic development, and institutional effectiveness, highlighting the macro-level implications of trust.

In contemporary empirical research, Edelman, through his Edelman Trust Barometer, conceptualizes it as the expectation that institutions government, business, the media, and NGOs will act competently, ethically, and in the public interest [7].

This definition reflects a normative and evidence-based understanding of trust, linking it directly to accountability, transparency, and ethical governance.

Empirical studies further confirm that trust is a key factor influencing the adoption and diffusion of innovations. Higher institutional levels are associated with increased willingness to adopt technological and policy innovations, as well as with a stronger perception of legitimacy [8], [9]. Furthermore, data from the European Commission, particularly through Eurobarometer, show that trust significantly influences public support for policies, technological transitions, and broader processes of social change [10].

Overall, public trust can be understood as a multidimensional construct that integrates cognitive, relational, and institutional dimensions.

The stance of key institutional sources on public trust

- ✓ The Organization for Economic Cooperation and Development emphasizes trust as a cornerstone of effective governance, linking it to transparency, accountability, and citizen engagement [8].
- ✓ The World Bank highlights trust as essential for policy implementation, institutional legitimacy, and economic development [9].
- ✓ The European Commission, through Eurobarometer, measures citizens’ trust in institutions and technologies across Europe, demonstrating its role in policy acceptance and social cohesion [10].

Furthermore, it is important to emphasize that “given the potential significant impact of AI on our society and the need to build trust, Europe has a duty to anchor its developments in this field in its values and fundamental human rights, such as human dignity and the protection of privacy. “On Artificial Intelligence - A European approach to excellence and trust” presents policy options that enable the reliable and secure development of AI in Europe while fully respecting the values and rights of European citizens.

The main building blocks of the White Paper are:

- ✓ the policy framework, which sets out measures to coordinate efforts at the European, national, and regional levels. It aims, through public-private partnerships, to mobilize the necessary resources

to build a “high-performance ecosystem” across the entire value chain, starting with research and innovation, and to create the right incentives for the accelerated deployment of AI-based solutions, including in small and medium-sized enterprises (SMEs);

- ✓ the key elements of a future regulatory framework for AI in Europe that will create a unique “ecosystem of trust.” [11].

In line with European values, fostering an environment of trust is viewed as a policy objective in its own right, aimed at addressing public concerns regarding the use of systems and applications based on artificial intelligence. At the same time, such an environment should provide the necessary legal predictability and certainty for businesses and public organizations when developing and implementing AI-based innovations. In this context, the European Commission consistently supports a human-centric approach to the development of artificial intelligence, in which technologies are oriented toward people, their rights, and their well-being. This approach is based on the principles for building trust in human-centric artificial intelligence and takes into account the practical experience gained and the recommendations formulated during the pilot implementation of the ethical guidelines developed by the High-Level Expert Group on Artificial Intelligence.

From a governance and communication perspective, it is grounded in key ethical factors such as integrity, reliability, and competence, which form the foundation for its development and maintenance. In this regard, Linda Hon and James E. Grunig make a significant contribution by developing a framework for measuring the relationships between organizations and their publics. They define trust as a central component of high-quality relationships, alongside variables such as satisfaction, commitment, mutual control, and shared values [12].

According to their model, it consists of three main dimensions:

- ✓ integrity – the belief that the organization is honest and fair;
- ✓ reliability – the expectation that the organization will fulfill its commitments;
- ✓ competence – the perception that the organization possesses the capacity to achieve its stated goals [12].

On this basis, a synthetic definition can be proposed: trust represents a relational assessment made by a trustor of a trustee in a specific context of uncertainty, where vulnerability is accepted based on the expectation of competent, ethical, and socially responsible behavior.

The comparison below is based on key literature reviews related to studies, management, and experimental research [13]. In an organizational and institutional context, trust is best understood not as a singular relationship, but as a structured architecture of reliability that can be designed, signaled, assessed, and, when necessary, repaired. Contemporary management research coalesces around several key pillars that collectively shape institutional trust.

The first pillar is governance capacity, referring to the ability of institutions to effectively perform their functions. Empirical data from the Organization for Economic Cooperation and Development show that perceptions of

reliability, responsiveness, and evidence-based decision-making are strongly associated with higher levels of public trust [14]. This reflects the dimension of reliability related to effectiveness, where trust depends on demonstrated competence and capacity to deliver. The second pillar is ethical governance, which refers to integrity, impartiality, and the appropriate use of power. Trust is strengthened when institutions are perceived as resistant to corruption, subject to checks and balances, and committed to the legitimate use of power. OECD findings further indicate that expectations regarding data protection, the integrity of public officials, and institutional accountability are critical determinants of trust [14].

The third pillar is procedural justice and legitimacy. Research on procedural justice, particularly by Tom R. Tyler, shows that people are more likely to accept decisions and cooperate with authorities when processes are perceived as fair, transparent, and respectful [15].

This underscores that trust is driven not only by results, but also by the way decisions are made and communicated.

The fourth pillar is the quality of communication. Strategic communication contributes to trust when it is timely, consistent, transparent, and dialogic. Research on transparency and communication shows that providing clear and substantive information increases trust, including in technology-mediated environments, such as interactions supported by artificial intelligence. In this sense, communication is not merely reputational but is constitutive of institutional legitimacy.

The fifth pillar is stakeholder engagement and voice. Trust increases when stakeholders perceive meaningful opportunities for participation, responsiveness, and dialogue, rather than one-way communication. Engagement frameworks emphasize that trust is built through observable inclusion, reciprocity, and responsiveness in decision-making processes.

The sixth pillar is the accountability framework, including corporate social responsibility (CSR) and, increasingly, corporate digital responsibility (CDR). Recent research conceptualizes CDR as a set of shared values and norms guiding organizational behavior regarding digital technologies and data management, extending accountability into areas such as privacy, algorithmic accountability, and the ethical use of artificial intelligence [16].

In technology-mediated societies, trust is no longer limited to interpersonal or institutional relationships; it extends to interactions between people, technologies, and institutions. This transformation positions it as a key prerequisite for:

- ✓ the adoption of digital innovations;
- ✓ the legitimacy of artificial intelligence governance;
- ✓ the sustainability of technological systems.

In this way, trust becomes a connecting mechanism between technological complexity and societal sustainability, reinforcing its role as a key factor for sustainable development in the digital age.

An analysis of contemporary research in the fields of corporate social responsibility, the green transition, and human resource management highlights a number of

established best practices that support the sustainable development of organizations through expert management.

First, there is a clear integration of sustainability into strategic management, whereby environmental and social goals are incorporated into organizational policies and management processes [17], [18]. This approach is linked to the transition from traditional corporate social responsibility to ESG-oriented models and social entrepreneurship.

Second, green human resource management (Green HRM) plays an important role in promoting sustainable organizational behavior through employee training, motivation, and engagement [19].

Particular attention is given to the development of so-called *green-collar workers* as a key resource in the context of the green transition [20].

Third, digitalization and the development of a digital culture are increasingly viewed as a source of competitive advantage, supporting effective human capital management and organizational adaptability in a dynamic environment [21], [22]. Thus, digital competencies and technological literacy are emerging as critical factors for sustainability.

Fourth, organizational culture and leadership are identified as key mechanisms for implementing sustainable practices, with employee motivation and values-based management contributing to the development of long-term organizational commitment [23].

Fifth, emerging technologies such as artificial intelligence, virtual and augmented reality (VR/AR), blockchain, and the Internet of Things (IoT) are having a significant impact on the tourism industry, transforming both the customer experience and business models. In this context, organizations are encouraged to embrace innovation strategically, invest in the development of digital competencies, and ensure the ethical and responsible use of technology. The future of tourism will depend not only on technological progress but also on the industry's capacity for flexible and sustainable adaptation [24].

Based on the analysis, the following applied trends can be identified within a technology- and sustainability-oriented trust-building framework:

- ✓ Integration of ESG principles into organizational strategies, with a focus on transparency, accountability, and long-term sustainability;
- ✓ Development of green human resource management (Green HRM) practices aimed at promoting environmental awareness and pro-sustainability behavior among employees;
- ✓ Investment in digital culture and competencies as a prerequisite for adaptability and innovation;
- ✓ Promoting leadership based on values and trust that supports organizational sustainability;
- ✓ Developing communication strategies that address misinformation and strengthen public trust in transformation processes [25];

- ✓ Embracing information security as a strategic tool for building trust, as effective data protection mechanisms are directly linked to the perceived reliability and legitimacy of digital systems [26];
- ✓ Implementing responsible communication practices, widely emphasized in professional codes of ethics, as a foundational element of the organizational vision and as a key tool in the execution of strategic and tactical communication plans [27].

Best practices such as integrating sustainability into management, developing green human resources, and digital transformation demonstrate that organizational sustainability is not merely a technological or economic process, but rather a social one...

A deeply constructed phenomenon in which the connecting mechanism between strategies, people, and results is the sustainability of trust. This gives rise to integrated practices at multiple levels, where ethics, communication, and management function as interconnected mechanisms. At the macro level, this is reflected in institutional frameworks and societal processes that collectively build sustainable and reliable systems, while at the micro level it manifests itself through organizational policies and behavior.

CONCLUSIONS

In this complex and dynamic field of research, a variety of concepts and analytical approaches are emerging that must be integrated into a coherent and organic framework capable of serving as a guiding reference point between technological development, sustainability, and a human-centered approach aimed at higher levels of trust. In this sense, technologies cannot be understood solely as tools for efficiency, innovation, and economic growth. They require a social and human dimension grounded in ethics, responsibility, inclusion, and institutional trust.

In practice, the accelerated pace of technological progress often outpaces the capacity of states and institutions to establish adequate regulatory frameworks to protect citizens. This creates tension between innovation and regulation, between technological efficiency and social security, and between digital progress and human rights. The digital sphere is increasingly intertwined with real-world experiences, significantly shaping the way people perceive the world, build their life experiences, and assess their own capabilities.

A sense of security, both in the present and regarding future prospects, is directly dependent on how technologies are managed, communicated, and regulated. In this context, a number of critical challenges arise, particularly regarding the blurred lines between voluntary participation and hidden coercion in digital environments. Practices that are formally based on user consent often raise questions about the extent to which that consent is truly informed and freely given, thereby creating conditions for what might be described as a "moral appropriation" of rights, even in the absence of explicit legal violations.

This, in turn, generates new dimensions of mistrust that extend beyond concerns about data security and encompass issues related to individual autonomy, dignity, and freedom.

At the same time, the influence of global technology players is growing, concentrating significant power within the digital ecosystem. In this environment, the need for greater transparency, accountability, and shared responsibility is becoming increasingly pronounced, with users no longer merely passive objects of technological processes but active participants and, to some extent, co-creators in their development.

The role of regulation is also being rethought, highlighting the need for multi-layered governance in which not only governments but also organizations, civil society, and consumers themselves act as arbiters and guarantors of trust. In this sense, if the logic of coercion replaces the logic of trust in everyday digital life, the risks extend beyond technological or economic consequences. Fundamental values such as human dignity, freedom, and social cohesion are at stake.

For this reason, the contemporary debate on technological and digital transformation must move beyond the narrow framework of economic efficiency and refocus on human well-being and social development as pathways to sustainability.

In summary, trust in technology can be conceptualized as a multidimensional construct encompassing competence, benevolence, integrity, transparency, predictability, and security. It is precisely the integration of these elements, supported by effective approaches and best practices, that enables technology to fulfill its primary function: improving the quality of human life without generating additional uncertainty or social tension.

Furthermore, the “human-centered” paradigm is closely linked to the concept of Society 5.0, which envisions an integrated system in which the digital, physical, and social spheres converge in a balanced and inclusive manner [28]. Within this framework, sustainable development cannot be achieved solely through technological progress but requires a holistic approach that combines innovative technological solutions with robust strategic and regulatory frameworks, as well as strong cross-sectoral partnerships.

The transition to sustainability, initiated by the UN 2030 Agenda and its Sustainable Development Goals (SDGs), has already generated visible impacts across all sectors and in most social and economic spheres of human life [20]. These transformations further reinforce the need to align technological progress with public expectations, ethical principles, and long-term sustainability goals.

In this context, the concept of “trust” emerges as a critical integrative mechanism that enables the effective coordination of technological innovations, governance structures, and social systems, thereby supporting the transition to a more inclusive, sustainable, and resilient Society 5.0.

Finally, it should be noted that the arguments presented are not devoid of the author’s perspective, reflecting an interpretive approach to the issue at hand. This stance, however, is explicitly acknowledged and is intended to stimulate critical academic debate regarding the role of trust as a central mediator between technological progress and sustainable development.

REFERENCES

- [1] IBM, “What is zero trust?” [Online]. Available: <https://www.ibm.com/think/topics/zero-trust> Accessed: Apr. 27, 2026].
- [2] Google Cloud, “What is zero trust?” [Online]. Available: <https://cloud.google.com/learn/what-is-zero-trust> [Accessed: Apr. 27, 2026].
- [3] Richard Edelman, “Insularity: The Next Crisis of Trust,” Edelman, 2026. [Online]. Available: <https://www.edelman.com/newsroom/richard-edelmans-6am-blog/insularity-next-crisis-trust>. [Accessed: Apr. 2, 2026]
- [4] Edelman, Edelman Trust Barometer 2026: Global Report, Edelman Data & Intelligence, 2026. [Online]. Available: [https://www.edelman.com/sites/g/files/aatuss191/files/2026-01/2026%20Edelman%20Trust%20Barometer%20Global%20Rep ort_01.21.26_0.pdf](https://www.edelman.com/sites/g/files/aatuss191/files/2026-01/2026%20Edelman%20Trust%20Barometer%20Global%20Report_01.21.26_0.pdf). [Accessed: Apr. 11, 2026].
- [5] N. Luhmann, *Trust and Power*. Chichester: John Wiley & Sons, 1979.
- [6] F. Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press, 1995.
- [7] Edelman, 2024 Edelman Trust Barometer: Global Report, Edelman, 2024. [Online]. Available: <https://www.edelman.com/trust/2024/trust-barometer>. [Accessed: Apr. 27, 2026].
- [8] Organisation for Economic Co-operation and Development (OECD), *Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions*. Paris: OECD Publishing, 2022. [Online]. Available: <https://doi.org/10.1787/b407f99c-en>. [Accessed: Apr. 27, 2026].
- [9] World Bank, *World Development Report 2017: Governance and the Law*. Washington, DC: World Bank, 2017. [Online]. Available: <https://doi.org/10.1596/978-1-4648-0950-7>. [Accessed: Apr. 27, 2026].
- [10] European Commission, *Eurobarometer: Public Opinion in the European Union, 2023*. [Online]. Available: <https://europa.eu/eurobarometer>. [Accessed: Apr. 27, 2026].
- [11] European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*. <https://op.europa.eu/bg/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1> [Accessed: Apr. 29, 2026].
- [12] L. Hon and J. E. Grunig, *Guidelines for Measuring Relationships in Public Relations*. Gainesville, FL: Institute for Public Relations, 1999. https://instituteforpr.org/wp-content/uploads/Guidelines_Measuring_Relationships.pdf. [Accessed: Apr. 21, 2026].
- [13] Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on Measuring Trust, 2017*. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/report_s/2017/11/oecd-guidelines-on-measuring-trust_g1g7ca1c/9789264278219-en.pdf. [Accessed: Apr. 3, 2026].
- [14] Organisation for Economic Co-operation and Development (OECD), *Drivers of Trust in Public Institutions 2024 Results, 2024*. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/report_s/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf. [Accessed: Apr. 3, 2026].
- [15] T. R. Tyler, *Why People Obey the Law*. Princeton, NJ: Princeton University Press, 2006.
- [16] T. T. Herden, E. Alliu, A. Cakici, et al., “Corporate digital responsibility,” *Journal of Business Research*, vol. 122, pp. 870–888, 2021. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8250868/>. [Accessed: Apr. 11, 2026].
- [17] I. Gigauri and V. Vasilev, “Corporate Social Responsibility in the Energy Sector: Towards Sustainability,” in *Energy Transition*, pp. 267–288, 2022.
- [18] I. Gigauri and V. P. Vasilev, “Paradigm shift in corporate responsibility to the new era of ESG and social entrepreneurship,” in *Sustainable Growth and Global Social Development in Competitive Economies*, pp. 22–41, 2023.

- [19] V. Vasilev, D. Stefanova, and M. Icheva, "Green human resource management as a component of sustainable organizational development," in *ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings*, 2024.
- [20] S. Yıldırım and V. Vasilev, "The Future of Green Collar Workers: Green Transition in Employment," in *Green Transition Impacts on the Economy, Society, and Environment*, S. Yıldırım, D. Yıldırım, I. Demirtaş, and V. Kandpal, Eds. IGI Global Scientific Publishing, 2024, pp. 1-16. doi: 10.4018/979-8-3693-3985-5.ch001.
- [21] V. Serafimova and V. Vasilev, "Digital culture as a competitive advantage in the sustainable development of organizations," *AGORA International Journal of Economical Sciences*, 2024.
- [22] V. Vasilev, D. Stefanova, and C. Popescu, "Human capital management and digitalization – From good practices and traditions to sustainable development," 2023. <https://doi.org/10.1108/978-1-83753-190-520231004>
- [23] V. Vasilev and I. Efremovski, *Organizational Culture and Employee Motivation – Theoretical Foundations and Best Practices*. Sofia: Propeler, 2017.
- [24] M. Modeva, "Opportunities and advantages of the application of artificial intelligence in tourism," *Multidisciplinary Journal of Science, Education and Art*, 2025.
- [25] D. Stefanova, K. Bacheva, and V. Vasilev, "Conceptual convergence: Disinformation, fake news, and information influence as a triad of security threats in the context of Society 5.0," in *ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference*, vol. 5, pp. 291–296, 2025. [Online]. Available: <https://doi.org/10.17770/etr2025vol5.8470>. [Accessed: Apr. 27, 2026].
- [26] K. Rannenberg, D. Royer, and A. Deuker, *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin: Springer, 2009.
- [27] M. Yankova, "Transparency in public relations activities – a fundamental principle for effective communication and building public trust," *Yearbook of the Department of Philosophical and Political Sciences*, vol. XIV/2024, pp. 49–55, Blagoevgrad: University Press "Neofit Rilski," 2024. ISSN 2683-0973. [Online]. Available: <http://press.swu.bg/images/yearbooks/%D0%93%D0%9E%D0%94%D0%98%D0%A8%D0%9D%D0%98%D0%9A%20%D0%BA%D0%BD.%202024.pdf> [Accessed: Apr. 11, 2026].
- [28] D. P. Stefanova, V. P. Vasilev, and I. P. Efremovski, "Re-Innovative Organizational Design: Sustainable Branding and Effective Communication - Applied Models in a World With New Borders/Without Borders," in *Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing*, pp. 112–127, 2023. doi: 10.4018/978-1-6684-8681-8.ch006. Available: <https://www.igi-global.com/gateway/chapter/325452#pnlRecommendationForm>. [Accessed: Feb. 11, 2025].

A Survey on Cyberbullying in Small and Medium-Sized Hi-Tech Enterprises in the Republic of Bulgaria

Ivaylo Ts. Stoyanov

Management in communications Department, University of
Telecommunications and Post, Sofia, Bulgaria
i.ts.stoyanov@utp.bg

Gergana Sl. Dimcheva

Management in communications Department, University of
Telecommunications and Post, Sofia, Bulgaria
g.dimcheva@utp.bg

Abstract — Digital technologies create conveniences for work and interaction of the human factors in an online environment, but at the same time, problems arise when using them. The integration of digital technologies into the business practice of hi-tech enterprises is a natural process through which the human factors communicates and creates business content. Since a large part of communication processes are carried out online and physical interaction between people decreases, the opportunities for unregulated use of ICT technologies are increasing. This communication connectivity through computer networks, software platforms, social media and mobile devices creates prerequisites for cyberbullying in the workplace. The publication has conducted a preliminary study on the impact of cyberbullying in an online environment and the consequences for the emotional and psychological state and health of people. Small and medium-sized hi-tech enterprises on the territory of three large cities in the Republic of Bulgaria were studied, using a quantitative approach in the development of an online survey through which empirical data was generated. Based on the results, an analysis of the manifestation of cyberbullying was conducted in order to identify its impact and consequences for the human factors in a working environment.

Keywords—Behavior, cyberbullying, hi-tech, human factors.

I. INTRODUCTION

With the development of Industry 4.0 and the transition to 5.0, enterprises are faced with the challenges of digital transformation of business (especially in the field of high technology), where various aspects of digital processes, AI, robotics, software, cloud solutions and others are part of the modern business process. As a result of the digital transformation of corporate processes, enterprises rethink the business model, switch to a digital strategy and corporate culture, implement new technological solutions,

tools and approaches to work in a digital environment [1], [2], [3], [4]. The choice of cutting-edge technologies for digital transformation of business requires hi-tech enterprises to create new ways of working and interacting in a digital environment. In order to remain competitive and achieve the desired efficiency in the conditions of digital transformation, they must rethink business processes for creating value, relationships with customers and stakeholders.

Unlike the traditional corporate office where bullying can occur through direct interaction between people working there, the development of cutting-edge technologies removes the boundaries of this physical interaction [5], [6], [7]. Now, through the impact of computer technologies and applications, people can communicate with each other in the workplace without meeting in physical interaction. The boundaries between bullying that occurs in a physical environment of human interaction and cyberbullying are clearly recognized. This distinction is important to emphasize the increasing role of cyberbullying with the accelerated development of technologies and the integration of professional and personal communication in an online environment. Some authors [8], [9], [10], [11] emphasize the specificity of these circumstances as an important fragment for studying the role and effects of cyberbullying in the modern workplace. According to them, traditional bullying, which is carried out through direct contact between people, has clearer indications for identification and taking adequate countermeasures. This is because it is easily recognized by the personal identity of the confronting parties, who are in physical contact with each other, and is difficult to establish as a result of the dynamics and rhythm of the existing conflict. On the other hand, cyberbullying is not only within working hours, it is permanent and constant,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.89>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

regardless of distance and is not always carried out by the persons who carry it out. They can hide their identity under foreign or fictional profiles and is often not limited to the interests and behavior of the affected parties. One of the features of cyberbullying is the access of data and information to the mass audience, which may be sympathetic to the existing conflict. Sharing, liking, rejecting or commenting on the relevant information can spread so quickly on the network that it creates a viral effect in the created negative situation. Often, cyberbullying leaves some kind of trace within the technology and applications through which it is used, which can be grounds for taking judicial or legal action when it is not compromised with profiles that do not correspond to the actual person (or group of people) responsible for the cyberbullying.

Cyberbullying with the development of technologies has an increasingly global impact on the behavior and work capacity of human resources [12], [13]. The presence of specialized platforms for online sharing of corporate information, online messages, social forums, photo sharing and online content in general, provokes subjects to possible forms of cyberbullying [14] [15]. The root of the problem is not only professional relationships in an online environment, where people strive to prove themselves and compete with each other, but also personal perceptions, reactions and behavior, which can always affect someone's side. These online relationships are not only publicly accessible, but also create different attitudes in the target audience, which can exceed the permissible ethical norms and practices of communication and interaction in a digital environment. Although there is no universal definition of cyberbullying in the workplace (as a result of the different possibilities and circumstances for its occurrence), a concept has emerged in the scientific literature that is associated with a tendentious and continuous manifestation of intentional actions that are directed at a specific subject in an online environment. This is done through the use of modern information technologies, and more specifically digital devices such as desktop and laptop computers, tablets, smartphones, text and voice messages, online videos, websites, social media, blogs, chat rooms and tweets [16], [17], [18].

In this regard, authors [19], [20], [21], examine the different forms of cyberbullying that have a negative impact on the behavior and actions of the human factors in the workplace. In the general aspect of the problem, cyberbullying arises from sending, publishing or sharing inappropriate online content that can affect the dignity and personal views of people. This occurs through digital content that has a harmful negative, false or slanderous effect on someone else, who may feel affected by the situation and react according to his position and point of view. These actions often relate to sharing compromising or misleading information that does not correspond to reality or that embarrasses or humiliates people in the context in which it is sent. Therefore, some authors [22], [23], emphasize the individual forms of cyberbullying that

have their own specificity and way of manifestation. These forms concern the publication and sharing of negative or personally harmful online content, so that a certain person or group of people is intentionally affected. Another possibility for cyberbullying in the workplace is social media, which people use to share both professional and personal information (often the two are mixed). At this level, various opportunities for cyberbullying arise, as a result of professional and personal attacks, sharing negative online content or making malicious comments. It should be taken into account the sharing of false information online or without the knowledge and approval of the relevant subject, carrying out hacker attacks or sending emails with negative or offensive content. Also considered a form of cyberbullying is sending emails or text messages that do not fall within the standard working hours of people, especially if an immediate response or reaction is required from the person (or persons) for whom it is intended. It is not uncommon in the workplace when people's professional commitments or personal space are affected by the use of a fake online profile, indecent chat messages or the publication of indecent online content. There are also situations where online content is shared and communication is conducted on behalf of someone else, false statements, comments are spread or lies are used that aim to compromise a specific person or group of people in the enterprise. It is not to be underestimated to provoke a state that can lead the subject of cyberbullying to unconscious actions that endanger their own lives and the lives of others.

II. MATERIALS AND METHODS

The main objective of the publication is to conduct a survey among a certain group of respondents in hi-tech enterprises, which were randomly selected, in order to establish the level of cyberbullying in work practices, the consequences and effects on the human factors. The study was conducted on the territory of three large cities in the Republic of Bulgaria - Sofia, Plovdiv and Burgas, where a number of small and medium-sized enterprises in the field of high technology develop their activities.

The surveyed enterprises carry out business activities in two sectors of the hi-tech industry - information technology and telecommunications. The object of the study are respondents who fall into the category of technical specialists and administrative personnel. The study did not include managers from the different levels of the surveyed hi-tech enterprises in order to ignore the influence of power relations and to provide an objective idea of the degree and forms of bullying among people who more often fall into this category, i.e. employees and the relationships between them. It is also important to establish the consequences of cyberbullying that arise for the human factors and what their presence in the work and the relationships between them leads to.

The study was conducted for research purposes, the scope of which provides the necessary information to gain an idea of the typology and manifestation of cyberbullying

in a work environment with the option of expanding it in the future to a larger territorial area. A quantitative approach was adopted to conduct the study, and an online survey was compiled to collect data from respondents at an interval of two and a half months. The conducted study is part of separate stages of a larger project to study the impact of cyberbullying in different sectors of industry in the Republic of Bulgaria. A method of collecting information was chosen through an online survey, the key advantage of which is saving time and costs for conducting the study. The electronic survey was sent to 46 small and medium-sized hi-tech enterprises at random with the option to be completed only by employees. The division of enterprises is into two categories - twenty-one in the field of information technology and twenty-five in the field of telecommunications. The authors' goal is not to make a distinction between individual enterprises, but to study different areas of business in high technology and the influence of cyberbullying on the general performance and behavior of the human factors.

The completed and returned questionnaires were from 157 employees, representatives of 38 small and medium-sized hi-tech enterprises, due to the refusal of 8 of them to cooperate in the conducted study. The completion of the web-based questionnaire is in accordance with the voluntary consent of the respondents, while respecting the requirements for confidentiality, and the information obtained is used only in the form of a sociological sample for the development of the publication. Respondents are given the opportunity to answer anonymously about the possibilities of cyberbullying (or lack thereof). The study does not set age limits and gender division of employees, but seeks a comprehensive answer about the manifestation of cyberbullying and the effect it creates.

The survey is structured in six main questions so that respondents assess several components in the work environment – experience of cyberbullying, frequency of its manifestation, subject of influence of cyberbullying, form of cyberbullying, possible impact of cyberbullying on work and productivity and effect on the physical and emotional state of the human factors. Through the conducted study, the authors of the publication aim to reflect how digital technologies in the work environment (and often in personal relationships as a result) affect the interaction of the human factors in an online environment. On the other hand, an opportunity is sought to establish the prerequisites for cyberbullying in the workplace and the consequences for the emotional-psychological state and health of people in the studied small and medium-sized hi-tech enterprises.

III. RESULTS AND DISCUSSION

The results of the survey are formed by six main questions, the application of which in the online survey aims to provide a comprehensive assessment of the manifestation of cyberbullying in the surveyed hi-tech enterprises. The questions cover quantitative information that is sufficient to establish the perceptions of the

surveyed employees, as the structure of the questions allows for a comprehensive analysis of the impact and manifestation of cyberbullying and the effects on the physical and emotional state of the human factors in the surveyed enterprises. From the obtained results, a conclusion can be made based on the answers provided by the respondents. They are primary in nature, without being processed with statistical tools, so as to provide a comprehensive picture of the nature of cyberbullying in a certain group of small and medium-sized hi-tech enterprises on the territory of three large cities in the Republic of Bulgaria. The discussion on the individual questions of the survey is based only on the online answers received, without additional research or interviews with the respondents. This requires looking for a logical connection between the respondents' answers and justifying their perceptions regarding the main aspects, manifestation and effect of cyberbullying.

Figure 1 shows that a fairly large percentage of the surveyed respondents in the surveyed small and medium-sized hi-tech enterprises (83%) have experienced some form of cyberbullying, regardless of the degree and level of its manifestation. On the one hand, this is due to the widespread use of technological tools for work and communication, as well as an immediate connection between the communicating parties, but it also shows a worrying trend of a high percentage of experienced cyberbullying in the workplace or personal relationships as a result of the work performed. Whatever the circumstances, the fact that employees share the presence of cyberbullying (as evidenced by the high percentage) indicates that there is a problem in the mechanism of implementing work practices, monitoring ethical organizational standards or ineffective communication in professional relationships. It is not excluded that people communicate professionally or personally outside of working hours, where it is also possible for forms of cyberbullying to manifest themselves when mixing professional and personal relationships. At the same time, the rather low percentage of respondents who state that they have not experienced cyberbullying is striking, regardless of whether they are completely convinced of this (1%) or have hesitations on the issue (4%). It is also evident that 12% of the surveyed respondents cannot assess the situation, which generally means that they either do not recognize the symptoms of cyberbullying (and accordingly it has not affected them in any way) or fall into the category of those who have not experienced it. Even so, the high percentage of employees who have experienced cyberbullying is an indicative trend for the tangible impact of technology on people and perhaps problems in corporate work practices and interaction.

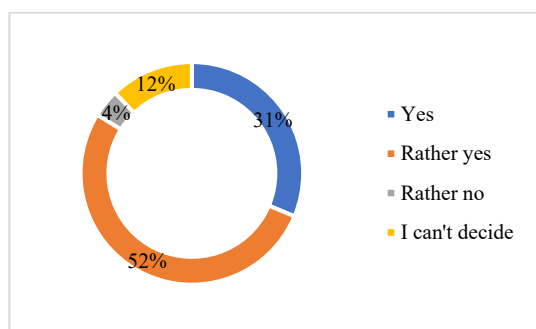


Fig. 1. Answer to the question: "Have you experienced cyberbullying at work"?

From Figure 2, it can be concluded that almost the entire group of respondents (91%) has experienced cyberbullying at work, although with different frequency of occurrence – constantly (31%), at a certain interval of time (43%) and occasionally (17%). In practice, this means that almost every employee at work has had situations of cyberbullying that have affected them in one way or another. The percentage of those who constantly experience cyberbullying is not small, which obviously has a different impact on the way in which work commitments are performed, including people being exposed to great risk regarding their physical and emotional state. This group is defined as risky because cyberbullying may increase as a trend, as a result of peculiarities in behavior and interaction between people or purely organizational problems in the activities of hi-tech enterprises. The highest percentage of the surveyed respondents is those who have received cyberbullying at work over a certain period of time, i.e. at cyclical intervals. This may be due to the development of group dynamics in the team or the attitude to work on various projects and tasks, which often exacerbate relationships in an online environment. Only 1% of respondents said that they had not experienced cyberbullying at work, and 8% of them could not assess the nature of the situation. In general, the authors' opinion prevails that regardless of the frequency of manifestation, cyberbullying in the studied hi-tech enterprises varies widely.

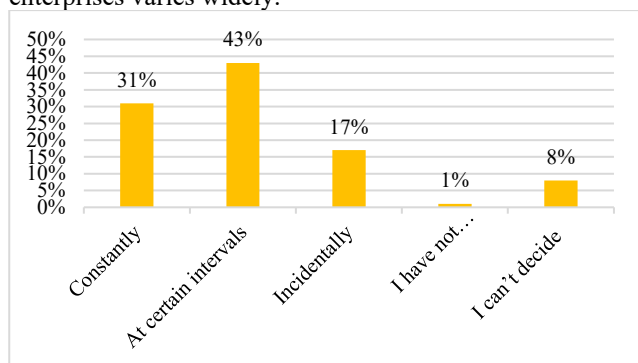


Fig. 2. Answer to the question: "How common is cyberbullying in the workplace"?

Figure 3 shows which subjects cyberbullying occurs in the workplace, according to the information from the surveyed group of respondents in hi-tech companies. It is striking that the largest percentage of cyberbullying is formed by work and interaction in the team or people who perform certain work duties together (59%). This may be due to various reasons that are related to daily communication and exchange of information between people, the way they communicate, distribute and fulfill their work commitments in an online environment. A large difference is also noted in the percentages of cyberbullying carried out by senior and direct managers – 2% and 31%, respectively. Perhaps this difference is normal and is explained by the access of employees to the relevant managers, i.e. the frequency and level to which they communicate with each other. It is normal for most communication and information exchange to take place with the immediate supervisor, resulting in cyberbullying situations in the workplace. The main reasons for this may be digital relationships at the expense of social ones, which are absent or neglected, unregulated mobile calls, email or chat messages outside of working hours, or other factors that oppose immediate managers and employees in an online environment. Since in most cases employees do not have access to senior managers or it is severely limited, cyberbullying amounts to only 3%. It should not be overlooked that not all actions of immediate managers fall into the category of cyberbullying (even if it appears to employees) when the rules for assigning, performing, reporting and controlling activities and tasks in an online environment are followed, which can be investigated in detail through another survey approach. 7% of respondents said they have experienced cyberbullying from customers, which in the context of digital business, online stores, websites and e-commerce platforms may be perceived as a normal phenomenon or at least not within the framework of the surveyed companies. When asked in the survey about the possibility of cyberbullying from business partners, there was no negative response (0%), which is due either to well-established relationships or employees having no contact with them.

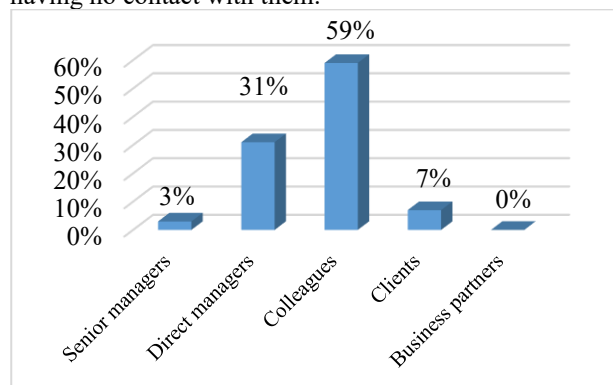


Fig. 3. Answer to the question: "Who have you been cyberbullied by at work"?

From Figure 4, a conclusion can be made about the form of harassment that respondents have experienced in the process of work and interaction in an online environment. It is striking that 87% of respondents claim to have experienced systematic cyberbullying on a personal basis. This also overlaps with a previous aspect of the study, mainly with regard to cyberbullying by colleagues. The main assumption here is that the constant interaction between people in the process of work is transformed into some personal relationships, which obviously mix with work and negatively affect not only communication, but also the result of the implementation of goals and tasks. The next point of a high percentage of cyberbullying from the study is online messages, mobile calls and chat outside working hours (73%). Perhaps this aspect of cyberbullying also overlaps with a previous question, mainly with regard to direct managers and their desire to achieve target goals and planned initiatives. Usually they are the ones who feel empowered to communicate with employees at any time of the day, regardless of the type of communication channel, which obviously reflects negatively on the respondents. More interesting is the case of cyberbullying based on indecent online and chat messages (45%). Here it is possible to make two main assumptions. First, collegial relationships at work are probably growing into personal ones (at least for one of the communicating parties), which is expressed in various forms of intimate or inappropriate conversations, including sending inappropriate photos. Second, with the development of technology, communication now dominates in an online environment, where, along with work relationships, personal ones also arise, which can cross the line of ethical and decent forms of behavior at work. Whatever the reasons, there is a lack of effective monitoring of the communication channel during work, unless this aspect of cyberbullying is mainly carried out outside of working hours, for which there is no clear indication. Also, 25% of respondents share about cyberbullying as a result of online messages and chat with fake content. A bigger problem is cyberbullying based on messages and chat with threatening content (11%), which is an obvious form of digital aggression. Management and cybersecurity experts in the surveyed hi-tech enterprises should implement a strict policy on digital online content and introduce systems and technologies for indicating malicious or provocative online practices. A part of the respondents reported cyberbullying through compromising devices for working with malware (3%), which is a cybersecurity lapse and another within 1%.

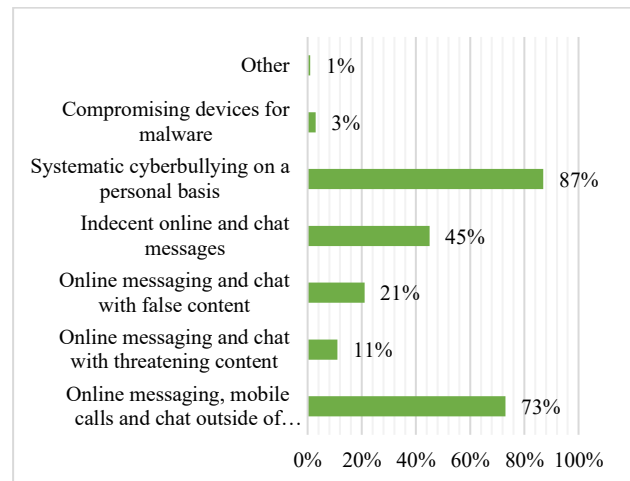


Fig. 4. Answer to the question: "What form of cyberbullying have you experienced at work?"

The question regarding the form of cyberbullying that employees have experienced at work is extremely interesting, as shown in Figure 5. For 83% of respondents, the problem arises from a lack of concentration, because cyberbullying distracts their attention from the real goals and tasks that they have to perform at work. An obvious consequence of this is low quality of work performed, as indicated by 76% of the employees surveyed. Another problem that arises among respondents as a result of cyberbullying is ineffective communication at work and the prerequisites that limit business communication between people (69%). It should not be forgotten that lack of concentration, low quality of work performed and ineffective communication are the main reasons for low productivity and efficiency. Approximately similar percentages of respondents are given that cyberbullying creates prerequisites for wasting time in performing work tasks (51%) and failure to meet deadlines (32%). Only 1% of respondents said that cyberbullying does not affect their work or their relationships with others, and 2% cited other reasons.

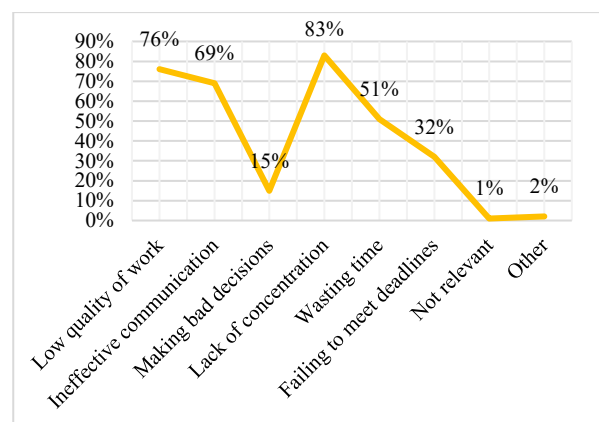


Fig. 5. Answer to the question: "How does cyberbullying in the workplace affect your work commitments and productivity?"

Regardless of the form and extent of cyberbullying, it can have different consequences for employees. Figure 6 shows how it affects their physical and emotional state in the hi-tech companies studied. The highest percentage of cyberbullying employees identify stress, anxiety and depression (91%), which is one of the major problems in the modern workplace, especially with the technologization of operations and the digital implementation of goals and tasks. Next in line are mental disorders (84%), health problems (78%), technostress from cyber provocations (68%), apathy and disinterest in work (35%). Only 1% of respondents claim that cyberbullying does not affect their work, and 4% indicated other reasons. These symptoms of cyberbullying should be regularly monitored, and senior management should take regular and adequate measures to implement strategies to counteract the negative effects.

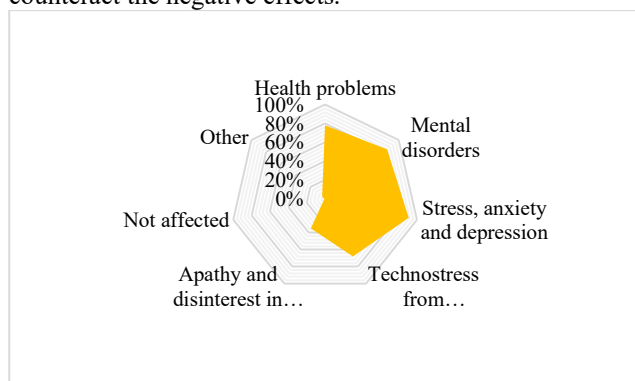


Fig. 6. Answer to the question: "How does cyberbullying affect your physical and emotional well-being?"

IV. CONCLUSIONS

The purpose of the publication was to study the presence of cyberbullying and its consequences on the human factors in small and medium-sized hi-tech enterprises in the Republic of Bulgaria. The publication generated results, the interpretation of which showed the presence of cyberbullying in the studied hi-tech enterprises, which is mainly due to the unprecedented use of technologies and software applications in work practices and communication between people. On the other hand, there is a lack of adequate mechanisms for prevention and deterrence in the online environment. It was found that employees experience cyberbullying constantly and at certain intervals of time and are practically affected by its manifestation in one way or another. From the point of view of the subject of influence, cyberbullying in the workplace occurs to the greatest extent as a result of group dynamics and the concentration of relationships within the team. The other more significant problem in this regard arises from direct managers who influence the behavior and actions of employees in the online environment.

Employees were affected by various effects, mainly due to systematic cyberbullying, which was carried out on a personal basis, including online messages, mobile calls

and chat outside working hours. From the point of view of the performance of work by employees, cyberbullying led to a decrease in productivity and distraction from their main tasks, including unfinished ones. The negative effects of cyberbullying are mainly manifested in a lack of concentration at the workplace, low quality of work performed, ineffective communication, as a result of which people waste unnecessary time in performing their assigned tasks and miss established deadlines. The negative effect of cyberbullying is that it affects the physical and emotional state of the human factors in the studied hi-tech enterprises, causing stress, anxiety and depression, mental disorders, health problems and technostress.

In addition, the reasons for the manifestation of cyberbullying are the lack of adequate mechanisms on the part of hi-tech enterprises for the prevention and monitoring of cyberbullying. In the general context of the issue, it has been established that cyberbullying is harmful (unwanted) behavior in the workplace, which can disrupt the personal and professional rhythm of any person exposed to stressful and harmful factors and situations in the online space. The empirical data in the publication can serve the authors for future research to establish the specific features of the types of bullying by categories of its manifestation and the role of direct managers in influencing subordinates. It is also necessary to study the factors that are a prerequisite for cyberbullying or are part of the employees' job commitments, as well as the indicators that form an inappropriate culture leading to cyberbullying in the workplace.

ACKNOWLEDGMENT

This research was funded by supported in part by the Research and Development Activity at the University of Telecommunications and Post, Sofia, Bulgaria, Project Number 44/30.03.2026.

REFERENCES

- [1] E. Martínez-Caro, J.G. Cegarra-Navarro, F. J. Alfonso-Ruiz, "Digital technologies and firm performance: The role of digital organisational culture", *Technological Forecasting and Social Change*, 2020, Vol. 154, [Online]. Available IDEAS, <https://ideas.repec.org/a/eee/tefoso/v154y2020ics0040162519312193.html> [Accessed: Apr. 2, 2026], <https://doi.org/10.1016/j.techfore.2020.119962>
- [2] V. Tuukkanen, E. Wolgast, L. Rusu, "Cultural values in digital transformation in a small company", *Procedia Computer Science*, 2022, Vol. 196, pp. 3-12, [Online]. Available ScienceDirect, <https://www.sciencedirect.com/science/article/pii/S1877050921022055> [Accessed: Mar. 23, 2026], <https://doi.org/10.1016/j.procs.2021.11.066>
- [3] G. Deep, "Digital transformation's impact on organizational culture", *International Journal of Science and Research Archive*, 2023, Vol. 10, pp. 396-401, [Online]. Available STUDOKU, <https://www.studocu.vn/vn/document/university-of-economics-hcmc/business-english/digital-transformations-influence-on-org-culture-insights-strategies/159891768> [Accessed: Apr. 5, 2026], <https://doi.org/10.30574/ijrsra.2023.10.2.0977>
- [4] J. Dooley, J. Pyżalski and D. Cross, "Cyberbullying versus face-to-face bullying: A theoretical and conceptual review", *Zeitschrift für Psychologie/Journal of Psychology*, 2009, Vol. 217(4), pp. 182-188, [Online]. Available APA PsycNet,

- <https://psycnet.apa.org/record/2010-01097-003> [Accessed: Apr. 5, 2026], <https://doi.org/10.1027/0044-3409.217.4.182>
- [5] L. Hauge, A. Skogstad and S. Einarsen, "Individual and situational predictors of workplace bullying: Why do perpetrators engage in the bullying of others?", *Work & Stress*, Vol. 23 (4), pp. 349-358, 2009, [Online]. Available ACADEMIA, https://www.academia.edu/20424733/Individual_and_situational_predictors_of_workplace_bullying_Why_do_perpetrators_engage_in_the_bullying_of_others [Accessed: Mar. 30, 2026], <https://doi.org/10.1080/02678370903395568>
- [6] M.A. Ciby and S. Sahai, "When and why workplace cyberbullying influences intention to stay: Role of workplace social capital and affective commitment", *International Journal of Manpower*, 2024, Vol. 45, No. 1, pp. 109-132, [Online]. Available Emerald, <https://www.emerald.com/ijm/article-abstract/45/1/109/141943/When-and-why-workplace-cyberbullying-influences?redirectedFrom=fulltext> [Accessed: Mar. 25, 2026], <https://doi.org/10.1108/IJM-04-2022-0183>
- [7] Y. Alahmad and H. Bata, "Cyber workplace bullying: An empirical study", *American Journal of Industrial and Business Management*, Vol. 11, pp. 767-784, 2021, [Online]. Available Scientific Research, <https://www.scirp.org/journal/paperinformation?paperid=110750> [Accessed: Apr. 3, 2026], <https://doi.org/10.4236/ajbm.2021.117048>
- [8] J. Platts, L. Coyne and S. Farley, "Cyberbullying at work: An extension of traditional bullying or a new threat?", *International Journal of Workplace Health Management*, 2023, Vol. 16 (2/3), pp. 173-187, [Online]. Available White Rose Research, <https://eprints.whiterose.ac.uk/id/eprint/199086/3/Traditional%20and%20cyberbullying%20paper%20revision.pdf> [Accessed: Apr. 2, 2026], <https://doi.org/10.1108/ijwhm-07-2022-0106>
- [9] N. D'Souza, D. Forsyth and K. Blackwood, "Workplace cyber abuse: Challenges and implications for management", *Personnel Review*, 2021, Vol. 50, No. 7/8, pp. 1774-1793, [Online]. Available Emerald, <https://www.emerald.com/pr/article-abstract/50/7-8/1774/331330/Workplace-cyber-abuse-challenges-and-implications?redirectedFrom=fulltext> [Accessed: Mar. 18, 2026], <https://doi.org/10.1108/PR-03-2020-0210>
- [10] E. Marsh, E.P. Vallejos and A. Spence, "The digital workplace and its dark side: An integrative review", *Computers in Human Behavior*, 2022, Vol. 128, 107118, [Online]. Available ScienceDirect, <https://www.sciencedirect.com/science/article/pii/S0747563221004416> [Accessed: Mar. 19, 2026], <https://doi.org/10.1016/j.chb.2021.107118>
- [11] Y. Wang, "Understanding the role of social factors in cyberbullying at work", *Computers in Human Behavior*, 2022, Vol. 134, 107325, [Online]. Available ACM Digital Library, <https://dl.acm.org/doi/10.1016/j.chb.2022.107325> [Accessed: Apr. 6, 2026], <https://doi.org/10.1016/j.chb.2022.107325>
- [12] W. Heatherington and I. Coyne I "Understanding individual experiences of cyberbullying encountered through work", *International Journal of Organization Theory & Behavior*, 2014, Vol. 17 No. 2 pp. 163-192, [Online]. Available Emerald, <https://www.emerald.com/ijotb/article-abstract/17/2/163/148272/Understanding-individual-experiences-of?redirectedFrom=fulltext> [Accessed: Mar. 27, 2026], <https://doi.org/10.1108/IJOTB-17-02-2014-B002>
- [13] C.S.L. Tan, "All by myself: Examining social media's effect on social withdrawal and the mediating roles of moral disengagement and cyberaggression", *European Journal of Marketing*, 2024, Vol. 58, No. 2, pp. 659-684, [Online]. Available Emerald, <https://www.emerald.com/ejm/article-abstract/58/2/659/1226349/All-by-myself-examining-social-media-s-effect-on?redirectedFrom=fulltext> [Accessed: Apr. 1, 2026], <https://doi.org/10.1108/EJM-12-2022-0932>
- [14] S. McCarthy, W. Rowan, C. Mahony and A. Vergne, "The dark side of digitalization and social media platform governance: A citizen engagement study", *Internet Research*, 2023, Vol. 33, No. 6, pp. 2172-2204, [Online]. Available Emerald, <https://www.emerald.com/intr/article-abstract/33/6/2172/177451/The-dark-side-of-digitalization-and-social-media?redirectedFrom=fulltext> [Accessed: Mar. 19, 2026], <https://doi.org/10.1108/INTR-03-2022-0142>
- [15] S. Adikaram, R. M. Dushmanthi and K. Ratnayake, "Making sense of cyberbullying: Stories of men and women at work", *Management and Labour Studies*, 2024, Vol. 49, pp. 568-589, [Online]. Available SAGE Journals, <https://journals.sagepub.com/doi/10.1177/0258042X241237040> [Accessed: Apr. 7, 2026], <https://doi.org/10.1177/0258042X241237040>
- [16] S. Farley, I. Coyne and P. D'Cruz, "Cyberbullying at work: Understanding the influence of technology", In P. D'Cruz, E. Noronha, E., Notelaers and G., Rayner, C. (Eds) *Concepts, Approaches and Methods. Handbooks of Workplace Bullying, Emotional Abuse and Harassment*, vol 1. Springer, Singapore. [Online]. Available Springer Nature, https://link.springer.com/rwe/10.1007/978-981-13-0134-6_8 [Accessed: Apr. 3, 2026], https://doi.org/10.1007/978-981-13-0134-6_8
- [17] S. K. Pothuganti, "Workplace cyberbullying: a systematic literature review on its definition, theories, and the role of HRD", *Cogent Business & Management*, 2024, Vol. 11(1), [Online]. Taylor & Francis, <https://www.tandfonline.com/doi/full/10.1080/23311975.2024.2408443> [Accessed: Apr. 1, 2026], <https://doi.org/10.1080/23311975.2024.2408443>
- [18] R.M. Kowalski, S.P. Limber and A. McCord, "A developmental approach to cyberbullying: Prevalence and protective factors", *Aggression and Violent Behavior*, 2019, Vol. 45, pp. 20-32, [Online]. Available ScienceDirect, <https://www.sciencedirect.com/science/article/abs/pii/S1359178917303968> [Accessed: Mar. 18, 2026], <https://doi.org/10.1016/j.avb.2018.02.009>
- [19] A. Kintonova, A. Vasyaev and V. Shestak, "Cyberbullying and cyber-mobbing in developing countries", *Information and Computer Security*, 2021, Vol. 29, No. 3, pp. 435-456, [Online]. Available Emerald, <https://www.emerald.com/ics/article-abstract/29/3/435/225410/Cyberbullying-and-cyber-mobbing-in-developing?redirectedFrom=PDF> [Accessed: Apr. 2, 2026], <https://doi.org/10.1108/ICS-02-2020-0031>
- [20] L. Barbosa-Santillán, B. P. Guzman-Velázquez, T. Orozco-Aguilera and L. Flores-Pulido. "Unraveling cyberbullying dynamics: A Computational framework empowered by Artificial Intelligence", *Information*, 16, 2025, 80, [Online] Available MPDI, <https://www.emerald.com/ijotb/article-abstract/17/2/163/148272/Understanding-individual-experiences-of?redirectedFrom=fulltext> [Accessed: Mar. 25, 2026], <https://doi.org/10.3390/info16020080>
- [21] N. Aboobaker and V. Shanujas, "Towards a sustainable workplace: Investigating workplace cyberbullying and its relationship with employee wellbeing and intention to stay in remote and hybrid work settings", *International Journal of Productivity and Performance Management*, 2024, [Online] Available IDEAS, <https://ideas.repec.org/a/eme/ijppmp/ijppm-12-2023-0662.html> [Accessed: Apr. 2, 2026], <https://doi.org/10.1108/IJPPM-12-2023-0662>
- [22] M. Angelova and A. Zielińska-Chmielewska, "Algorithmic management in the digital transformation of enterprises: A qualitative study of motivations and strategic implications", *Economics, Ecology Socium*, 2025, Vol. 9, pp. 79-96, [Online] Available Economics Ecology Socium, <https://ees-journal.com/index.php/journal/article/view/319> [Accessed: Mar. 28, 2026], <https://doi.org/10.61954/2616-7107/2025.9.4-6>
- O. F. Malik and S. Pichler, "Linking Perceived Organizational Politics to Workplace Cyberbullying Perpetration: The Role of Anger and Fear", *Journal of Business Ethics*, 2022, 1-19, [Online]. Available PMC PubMed Central, <https://pmc.ncbi.nlm.nih.gov/articles/PMC9443633/> [Accessed: Mar. 18, 2026], <https://doi.org/10.1007/s10551-022-05234-7>

The Role of Artificial Intelligence in Educational Technologies for the Purposes of Higher Education – Experimental Research

Zhaneta Tsoneva

Department of Social and Economic Sciences

Technical University of Gabrovo

Gabrovo, Bulgaria

janett_c@abv.bg

Abstract—This research focuses on the role of artificial intelligence in educational technologies in higher education. The modern vision and needs of current and future professions set new requirements for the training of future specialists related to the use and application of high-tech training resources. The relevance of the issues under consideration stems from the need to adapt the training to the modern requirements of professional practice. In Bulgaria, the application of artificial intelligence in higher education is developing rapidly, but there are areas where it is still in its early manifestation process. The purpose of this study is to analyze the development of educational technologies using artificial intelligence and to present the results of a pilot experimental study among students, aimed at upgrading the previously applied learning technologies by implementing artificial intelligence. The results of the experimental study show an increase in student motivation and learning efficiency using AI for learning purposes.

Keywords— artificial intelligence, educational technology, social work, training.

I. INTRODUCTION

In the era of new technologies in recent years, artificial intelligence has been rapidly establishing itself and has found application in numerous fields of professional practice. Several studies in recent years have attested to the implementation and use of artificial intelligence for the purpose of more effectively decision-making, demonstrating flexibility, and adapting to the new business and practical requirement. As Nikolova-Minkova points out “*people’s creativity has been a generator of their development and a prerequisite for high scientific and technical achievements, giving the appearance of modernity*” [1, p.243]

In the sphere of education, the interest of the impact and role of artificial intelligence is increasingly deepening and expanding, having in mind the unlimited possibilities that

AI provides. Several studies lay the foundation for numerous models generated in administration, educational technologies, and the use of training tools and resources. As Chain et al. point out, artificial intelligence enables the enhancement of teachers’ effectiveness and efficiency, makes possible the personalized approach to students, based on their needs and requirements, and consequently improves the quality of learning [2].

The term “*artificial intelligence*” has become firmly established in both the research and applied aspects of education. Globally, UNESCO, through the Education 2030 Program, seeks to promote a human-centered approach to AI, with the main priority of making innovative AI technologies accessible to all, while adhering to the principles of equality and inclusion [3]. Several regulatory documents provide guidance for the use of AI in educational sector. Their main objectives are to promote high-quality digital education and training [4], to develop digital competences through the creation of AI learning resources [5], and to establish ethical guidelines for the use of AI for educational purposes [6]. In Bulgaria, trends and strategies in the educational sector regarding the implementation and use of artificial intelligence for the purposes of the educational process, are focused on modern digital infrastructure [7], [8], interactive learning, digital resources, teachers’ trainings [9].

The purpose of this study is to examine the development of educational technologies utilizing artificial intelligence and to present the results of a pilot experimental study focused on the application of artificial intelligence in the learning process.

The object of the current study is the artificial intelligence. The subject of research is educational technologies generated by artificial intelligence.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.73>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

In the theoretical part of the article, educational technologies using artificial intelligence are examined, having in mind their development, contribution, and innovation for the purpose of training future specialists in various fields of professional activity. The empirical part of the publication presents the results of a pilot experimental study to determine the significance and role of educational technologies using artificial intelligence in the education of students. Through the research methods used -such as analysis, synthesis, experimentation, statistical methods and tabular presentation of data-, an attempt is made to illustrate the role of artificial intelligence in educational technologies for the purposes of higher education. Concluding with the summary of the research finding of the conducted study and outlining the future challenges that higher education will face by introducing educational technologies with artificial intelligence in students' training, the article emphasizes the significance of artificial intelligence in educational technologies and the need to continuously improve and adapt the educational system to the opportunities provided by artificial intelligence.

II. MATERIALS AND METHODS

A. Literature review

The expectations and requirements that society makes regarding the process and conditions of training future specialists in different professional spheres have constantly evolved throughout history, they are currently changing and will continue to change dynamically. This implies changes in the organization, technology, and the process of education. In this context, viewed historically, education as a process- including the methods and tools used- undergoes through various transformations and is determined by the dynamics of technological progress at both national and international levels.

Historical and pedagogical research on the ideas of regarding the interaction between a teacher and a learner supports the thesis that at the center of effective learning is the question "how" – what educational technologies, what tools and methods are appropriate and suitable for the specific situation or learner. A review of the literature sources on the subject shows that even in the distant past, the use of innovative technologies for the purposes of human learning was related to people's needs for more accessible, easier, and faster learning.

For the purposes of the research, it is interestingly to consider the definitions of the concept of "educational technology" from the point of view of their evolutionary development through a brief historical overview.

The early years of the 20th century were marked by the development of innovative solutions that shaped educational technologies. Using technological innovations such as projectors, slides, films, and visual learning in schools become not only more enriched, but also more

accessible, emphasizing on the experiences rather than more mechanical memorization [10, p.37]. Between the 1960s and 1980s, educational technology integrated the complex relationships between the organizational and managerial context of learning and educational resources (people, techniques, tools, environment) to address learning challenges [11], [12], [13]. The following years marked an expansion of the scope of the definition of educational technology toward a systemic -process approach. By integrating ideas from various sources ("conceptual" technologies) the best learning environment is ensured [14], furthermore educational technologies promote "intellectual development" and "continuous learning ability" [15, p.13]. In the context of the systematic examination of educational technology, according to Khutorskoy, the technology of education is "*a set of consistent and dynamic alternation of specific goals, content, procedures (methods), means (techniques), organizational forms, control and evaluation mechanisms and criteria for comparability of goals and results*" [16, p.82]. Similarly, the conceptual understanding of educational technology proposed by Januszewski and Molenda includes the combination of elements of *research* (improving and upgrading knowledge by exploring of new problem areas), *ethical practice* (commitment to and alignment of one's own ethical and professional conduct), *facilitation* (supporting learning through appropriate environments, resources and tools), and *productivity* (the ability to utilize and apply new opportunities with a focus on individuality) [17]. The information age makes information more accessible, anywhere and at any time, but it necessitates the need for a higher level of information literacy.

The contemporary perspective on educational technologies implies the upgrading of definitions, according to [18], in the direction of student empowerment and inclusion, ethical integration of technologies and a learner-oriented environment [see Fig. 1]. The Association for Education Communication and Technology (AECT) defines educational technology as "*the study and ethical practice of facilitating learning and improving performance by creating, using, and managing appropriate technological processes and resources*" [19, p.1]. In the cited article, the primary objective, highlighted in the definition, is learning and ethical practice, that is, the importance of teaching values, which is the focus and essence of educational technologies. The authors point out that the tools - means, resources, processes -are part of educational technology. The emphasis in the contemporary understanding of educational technology is also the concept, which is related to the inclusion and access to education for disadvantaged groups of the population. As Todino points out, educational technologies are key to ensuring equal access to learning and supporting the development of "*digital, cognitive, and critical skills, meeting the needs of a changing world.*" [20, p.1].

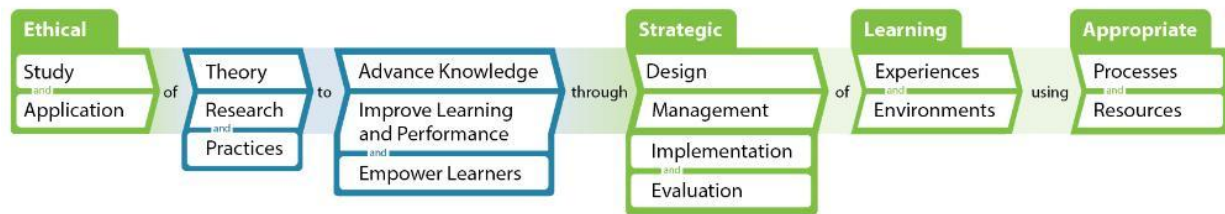


Fig. 1. Definition of educational technology [8, p.57]

Today, educational technologies are expanding the scope of their terminological interpretation, which is largely due to the development in recent years of technologies using artificial intelligence. The growing interest in researching the role, impact and implementation of artificial intelligence in various areas of the professional and educational spheres, reflects the significant role and place of innovative technologies and future projections for their development and implementation.

According to the generally accepted understanding, Artificial Intelligence (AI) is defined as a technology through which complex problems in specific situations can be solved. Most authors in recent years have accepted that definition artificial intelligence is complex and requires a more comprehensive examination not only in terms of the necessary skills, goals, tasks, and actions that artificial intelligence performs, but also a clearer understanding of the phenomena and processes that arise from its application [21], [22], [23]. The European Commission's High-Level Expert Group provides the following definition of artificial intelligence: "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" [24, p.1].

Similar to the periods of educational technologies development discussed above from a terminological perspective, here we examine the evolution and dynamics of the development of artificial intelligence in educational technologies. The early years (1950s-1980s) were marked by the emergence of the first AI concepts in education, which marked the beginning of Artificial Intelligence in Education (AIED). As early as 1950, Turing presented his concept of the "intelligent" aspect of systems by testing the ability to distinguish between a conversation with another person or a machine. According to him, if no such distinction is found, then an intelligent system (AI) is present [25]. Expert systems, adaptive and training programs such as PLATO (Programmed Logic for Automatic Teaching Operations), TICCIT (Time-Shared, Interactive Computer-Controlled Information Television) place the individual needs of learners [26], adaptability, and two-way interaction at the center of educational technologies and learning, and these implications remain relevant today. Over the next twenty years, the integration of more complex, intelligent education systems, the use of

analytical approaches and data-driven systems to improve personalization were observed. Since the year 2000, machine learning, large databases, and adaptive systems have evolved rapidly, and the field of AI research expanded. As Huang et al. points out, the focus is on the use of AI in learning technologies to support teaching, facilitate learning, "realize smart learning," through innovative smart resources such as virtual classrooms, adaptive learning, smart educational robots [27, p.207]. The accelerated pace of development and implementation of AI in educational technologies has been significantly influenced by the global Covid 19 pandemic. Due to epidemiological restrictions, educational institutions have switched to online learning and the use of digital resources, which require the adaptation and enhancement of knowledge, skills and competencies of both students and teachers. According to Vázquez-Cano, artificial intelligence in education in recent years can offer an opportunity to improve the quality of learning through a more sustainable model, in line with the recommendations of UNESCO's "2030 Agenda for Sustainable Development", by creating a more enriching and personalized learning environment, integrating AI into methods such as blockchain, gamification, conversational agents and others. [28, p.9]. The current stage of development and application of AI in educational technologies is determined by the outburst of research on generative AI, such as the GPT model, various hybrid models for human-machine learning, etc.

At the same time, significant attention is being paid to the ethics and social aspects of the application of AI in the educational environment. Today, the learning process and interaction between students and teachers is supported by the help of several innovative technologies generated with AI – Canva, virtual reality (VR) and augmented reality (AR), Microsoft Sway, etc. [29].

Based on a systematic review of publications between 2023 and 2024, Bang et al. note that unlike conventional digital educational tools, AI systems based on large language models (LLMs) provide the opportunity for interactive, adaptable, and personalized learning environments in real time [30]. Research in recent years has shown that the integration of ChatGPT and other AI Chatbot platforms into the educational process leads to an increase in motivation, engagement, and a higher degree of

personalization of students' learning [31]. The authors emphasize the contributions that AI tools have such as virtual academic assistant, automatic feedback, etc. At the same time, they point out that it is necessary to develop strategies to minimize shortcomings and change curricula in education in order to achieve a balance between knowledge, use and ethics [31, p.17]. The innovative capabilities of AI technologies are also manifested in their ability to change the pedagogical model from a teacher-centered to a learner-centered approach. Instead of inert perception of information and passive participation in the pedagogical situation, students actively interact with the system through an interactive form of organization of the educational process. This is in line with modern concepts of adaptive and personalized learning [32]. In addition, meta-analysis studies have found a positive effect on students' cognitive and non-cognitive skills, highlighting the innovative importance of AI technologies in improving academic achievement, autonomy, and student engagement [33]. Despite the positive results reported by recent meta-analysis, the researchers emphasize the importance of pedagogical control and responsible implementation of AI technologies to avoid overuse and superficial learning outcomes [34], [35].

In this context, the analysis of literature sources allows us to assume that the implementation of AI chatbot technologies in education can be perceived as an innovative approach that collaborates simultaneously personalization, automation, and interactivity in support of the development of modern educational practices. Current research shows that artificial intelligence in education has the potential to improve the learning process, but at the same time sets new requirements for the preparation of pedagogical models, digital literacy, and ethical standards in education.

Based on the literature review of the definition of the concept of “educational technology” and AI in educational technologies, the working definition that we adopt for the purposes of the study is as follows:

Educational technology is a purposeful process that is carried out in accordance with regulatory and ethical requirements, aimed at achieving educational goals, through the acquisition and development of competencies, using contemporary appropriate forms, methods and resources of training, with measurable results and systematic monitoring, influenced by the environment, learners and context (see Fig. 2).

B. Methodology of the research

The study used a quasi-experimental one-group pre-test/post-test design aimed at evaluating the educational effectiveness of simulated interaction scenarios supported by artificial intelligence in teaching social work students. The experimental approach was chosen due to the specific pedagogical context of social work education, where traditional teaching methods are mainly based on discussions, lectures, and theoretical case studies.

In the context of Bulgarian higher education in social work, the existing structure of the curricula is mainly focused on theoretical and disciplinary training. However,

opportunities for practical training and simulated professional interaction in the university learning environment remain relatively limited, especially with regard to the integration of interactive technologies supported by artificial intelligence.

The implemented AI-supported learning model introduced interactive scenario-based activities that allowed students to participate in simulated communication and decision-making processes. This represents an innovative pedagogical approach compared to conventional teaching.

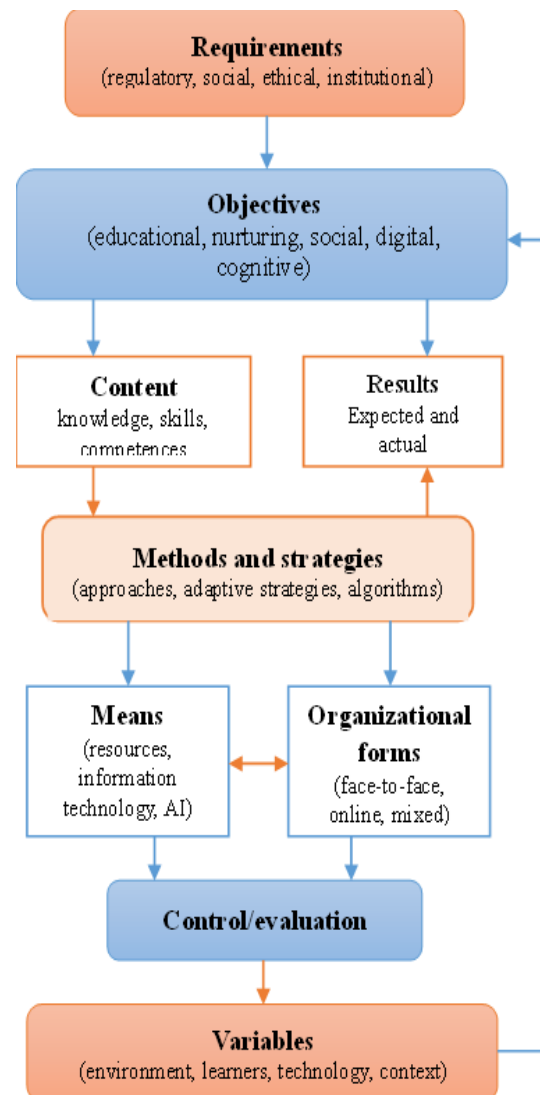


Fig. 2. Elements of educational technology [Own preparation]

The tasks by which we realize the purpose of the study are as follows:

1. To develop a training simulation method using AI for practical training.
2. To implement experiential learning by using a training simulation method with AI.
3. To analyze students' attitudes towards the new method of practical training.

The object of this experimental study is the training process for students majoring in “Social Activities” at the Technical University of Gabrovo, Bulgaria.

The subject of research is practical training using an AI-based simulation method as an innovative method.

The hypothesis of the study states: the implementation of AI-based simulation method in the practical training of students leads to statistically significant improvements in results and higher motivation.

The stages of the experimental study include:

1. Ascertaining stage, the purpose of which is to establish the initial level through the following methods: entrance test for knowledge and skills, survey for digital competence and motivation, observation.

2. Formative stage, the purpose of which is to apply a simulation method using artificial intelligence in the practical training of students.

3. Assessment stage, aimed at evaluating the impact of training, using the following methods: an exit test of knowledge and skills, structured in the same way as the entrance test; a survey of satisfaction and attitudes; comparative analysis of the results.

The experimental research methods used are single-group pedagogical experiment, a simulation based teaching method, knowledge and skills tests, questionnaires, observation, statistical analysis (t-test, Cohen’s d, percentage analysis).

The research was carried out in January 2026 among 15 students majoring in “Social Activities” at the Technical University of Gabrovo, Bulgaria. Students are in the third year, bachelor’s degree.

To collect the data necessary to test the hypothesis, we used the following tools:

1. A chatbot that we developed through the Soul Machines Ins platform and integrated into a training site created for the purpose of training students.

2. Entrance test to measure the students’ initial level of knowledge and counselling skills of students.

3. Survey to analyze the motivational component, digital readiness, and attitudes towards AI-based learning.

4. An exit test and a comparison survey with the baseline data, used to measure the cognitive effect, the development of counseling skills, the motivational effect, the perceived realism of the AI simulation.

Participants in the study take part voluntarily. All tools used are anonymized to ensure the protection of personal data and confidentiality.

III. RESULTS AND DISCUSION

We implemented the pilot study through a single-group pedagogical experiment with input and output measurement. Through knowledge and skills tests (Table

1) and digital competence and motivation surveys, we collected the necessary information for analysis.

By calculating the average, we determined the difference between the outgoing and incoming test (see Table 2), where $\bar{X}$ denotes the mean value and D shows the difference between the two tests.

The results show that after training by applying a simulation method with a chatbot, an increase of 8.34 points was observed, indicating a positive change in students’ knowledge and skills.

TABLE 1 ENTRY AND EXIT TEST DATA

Serial number student	O1 – Entry Test	O2 – Exit Test
S1	20	30
S2	25	30
S3	15	25
S4	15	25
S5	25	30
S6	20	30
S7	10	20
S8	15	20
S9	15	20
S10	10	20
S11	20	30
S12	20	25
S13	10	20
S14	15	25
S15	15	25
Σ	250	375

TABLE 2 ENTRY AND EXIT TEST RESULTS

	O1 – Entry Test	O2 – Exit Test
$\bar{X}$	16,66	25
$D = \bar{X}O1 - \bar{X}O2$	8,34	

The percentage increase (1) is approximately 50 % compared to the baseline calculated using the following formula

$$\frac{O_2 - O_1}{O_1} \times 100 = \frac{8,34}{16,66} = 50,06 \% \quad (1)$$

We analyzed the data from the survey through descriptive and comparative statistics. The results of the initial survey on students’ motivation and digital competence show that 60% of respondents feel motivated to develop conversation skills (counseling), but only 40% believe that they could have a consultative conversation with a client. Regarding their interest in innovative training methods such as chatbots, simulations, interactive

presentation systems, and others, half of the respondents (53.3%) reported increased interest. Students' digital competence regarding the use of AI tools (AI assistants, chatbots) for learning, working, and other purposes is high (60%), which confirms their motivation and interest. At the same time, however, respondents do not feel confident to conduct a text dialogue with a chatbot on their own (40%). The majority of students (60%) note in the initial survey that they expect to improve their skills in conducting consultative conversation after conducting simulation training with a chatbot.

The results of the post-training survey register the students' feedback on the training conducted. One of the key questions in the survey finds out whether the chatbot simulation recreates a consultative situation that is as realistic as possible. According to 66.6% of students, this type of simulation is very useful for training purposes and creates a sense of real-life experiences. The majority of respondents (73.3%) also share that after the simulation they feel more motivated and confident in conducting a consultative conversation, as well as that it helps them to recognize and validate the emotions of the client - a chatbot - more clearly. Taking into account the nature of the work of the helping specialists, including social workers, the awareness of one's own strengths and weaknesses is extremely important for the implementation of quality and effective work. In this regard, 60% of students share that this type of training helps them identify what aspects of their verbal and non-verbal communication and reactions contributed to the success of counselling session and what hindered it. 86.6% of respondents are adamant that the use of interactive teaching methods such as chatbot simulations and the like will be beneficial for students throughout the educational process in various disciplines. Their expectations are to provide more opportunities for applying AI in their education so that they can build on their knowledge with practical skills that closely resemble the real work environment.

To verify the statistical significance of the differences between the input and output measurement, we applied a t-test for dependent samples. The resulting difference between the two measurements is statistically significant ($t(14) = -13.23, p < 0.001$).

In addition to statistical significance, we also calculated the effect of the Cohen's d intervention on dependent samples. The obtained value ($d=1.25$) shows an exceptionally strong effect of learning through chatbot simulation on student performance.

The formulated research hypothesis, according to which the application of a simulation method using artificial intelligence in the training of students leads to a statistically significant improvement in results and an increase in learning motivation, is confirmed on the basis of the analysis of the data from the pilot experimental study.

The findings suggest that AI-supported simulated scenario-based learning can provide pedagogical advantages compared to conventional learning methods

often applied in social work education. Traditional teaching methods in this field, especially in Bulgarian social work education, limit students' opportunities for active experimental participation. In contrast, interactive pedagogical situations supported by artificial intelligence allowed students to participate in simulated professional interactions through which to practice communication, decision-making, and problem-solving skills in a more interactive and practice-oriented environment. The observed improvement in pre- and post-test scores indicates that integrating simulations using artificial intelligence can contribute positively to increasing students' motivation and engagement in learning.

The study is subject to several limitations. The experimental intervention was carried out within a single-group pre/follow-up test design, without a parallel control group, which limits the direct comparison with conventional discussion approaches in social work training. In addition, we conducted the study in a university setting and included a relatively specific student population, which may affect the applicability of the results in other educational contexts. However, the study offers initial empirical evidence on the applicability of simulated AI-supported interaction scenarios in practice-oriented higher education.

The innovation of the proposed approach lies not only in the use of the AI technology itself, but also in the fact that we have integrated simulated scenarios for professional interaction, supported by artificial intelligence, aimed at experiential and practical learning. In this regard, the research contributes to the growing volume of research on pedagogical models enhanced with artificial intelligence in higher education.

The results of the experimental study are in line with recent research on the integration of AI in social work education. Modern studies have found that AI-supported learning environments are useful and recommended for social work educators [36], [37]. Furthermore, studies focused on ethical dilemmas and professional decision-making have considered the potential of ChatGPT as a supporting tool in social work training, through which to develop skills such as effective communication, reflection, without replacing the human element of the profession [38].

Contemporary research highlights the need for balanced and pedagogically controlled integration of AI. A recent study highlighted the potential risks associated with over-reliance on AI technologies, especially in terms of reducing human interaction in educational environments [39]. Therefore, through the results of this study, we support the understanding that educational technologies using AI should be perceived as complementary tools and not replace the pedagogical role of the educator.

The proposed approach can be interpreted within the broader historical evolution of educational technologies, where a gradual transition from traditional learning models to interactive and practice-oriented learning environments is demonstrated. In this context, we believe that AI-

supported simulation learning is perceived as a modern stage in the integration of smart and experimental technologies in higher education in social work.

IV. CONCLUSION

The topic of AI in student education as part of educational technology is important for two main reasons. The first is related to the quality and effectiveness of education. The second arises from the need to implement and utilize new teaching methods in accordance with global trends and the evolution of future professions. The results of the study show that the use of interactive AI-based teaching methods, such as a chatbot simulation in students' education, increases their motivation and leads to higher results. This means that a more in-depth study of the potential of AI for educational purposes is needed, which could serve as a basis for future research.

REFERENCES

- [1] V. Nikolova-Minkova, "Historical development of technologies in the field of artificial intelligence," *Environment Technology Resources Proceedings of the International Scientific and Practical Conference*, vol. 2, pp. 243–250, Jun. 2025. [Accessed January 15, 2026], <https://doi.org/10.17770/etr2025vol2.8609>.
- [2] L. Chen, P. Chen and Z. Lin, "Artificial intelligence in education: A review," *IEEE access*, vol. 8, pp. 75264–75278, 2020.
- [3] UNESCO, "Artificial Intelligence in education," [Online]. Available: UNESCO, <https://www.unesco.org/en/digital-education/artificial-intelligence>. [Accessed January 19, 2026].
- [4] Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024, Official Journal of the European Union. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>. [Accessed January 20, 2026].
- [5] Digital education action plan (DEAP) (2021-2027), European Commission. [Online]. Available: European Commission <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>. [Accessed January 20, 2026].
- [6] The Institute for Ethical AI in Education, The Institute for Ethical AI in Education The Ethical Framework for AI in Education. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>. [Accessed January 20, 2026].
- [7] Ministry of Transport, Information Technology and Communications, Concept for the Development of Artificial Intelligence in Bulgaria until 2030, 2020. [Online]. Available: <https://www.mtc.government.bg/sites/default/files/conceptforthedevelopmentofaiinbulgariauntil2030.pdf>. [Accessed January 12, 2026].
- [8] D. Petrova, "Intelligent, innovative and sustainable industry in Bulgaria – prospects and challenges," *Environment Technology Resources Proceedings of the International Scientific and Practical Conference*, vol. 1, pp. 210–215, Jun. 2019. [Online]. Available at: <https://archive-journals.rtu.lv/etr/article/view/4210>. [Accessed March 28, 2026].
- [9] Ministry of Education and Science, Strategic Framework for Education, Training and Learning 2021–2030, 2021. [Online]. Available: <https://www.navet.government.bg/bg/media/strategicheska-ramka-obrobuuchene-110321-1.pdf>. [Accessed January 12, 2026].
- [10] M. Molenda, D. Subramony, R. Clark-Stallkamp, "A brief history of educational technology," in *Foundations of learning and instructional design technology: Historical roots & current trends*. EdTech Books, 2025. [Online]. Available: <https://edtechbooks.s3.us-west-2.amazonaws.com/pdfs/473/8731.pdf>. [Accessed January 14, 2026].
- [11] AECT Task Force, The definition of educational technology. Washington, DC, USA: Association for Educational Communications and Technology, 1977. [Online]. Available: https://ocw.metu.edu.tr/file.php/118/AECT_Definition_20of_20Educational_20Technology.pdf#. [Accessed January 14, 2026].
- [12] D. P. Ely, "The definition of educational technology: An emerging stability," *Educational Considerations*, vol. 10, no. 2, Apr. 1983. [Online]. Available: <https://doi.org/10.4148/0146-9282.1793>. [Accessed January 15, 2026].
- [13] R. M. Gagné, "Educational technology and the learning process," *Educational Researcher*, vol. 3, no. 1, pp. 3–8, Jan. 1974. [Online]. [Accessed January 22, 2026], <https://doi.org/10.3102/0013189X003001004>.
- [14] S. Hooper and L. P. Rieber, "Teaching with technology." in *Teaching: Theory into practice*, 2013, pp. 154–170, 1995. [Online]. Available: <file:///C:/Users/ZBook/Downloads/TeachingwithTechnologyHooperRieber1995-2.pdf>. [Accessed January 22, 2026].
- [15] A. Lakhana, "What is educational technology? An inquiry into the meaning, use, and reciprocity of technology," *Canadian Journal of Learning and Technology/La revue canadienne de l'apprentissage et de la technologie*, vol. 40, no. 3, 2014.
- [16] A. Khutoroskoy, *Modern didactics*, Saint Petersburg, Moscow, Russia, 2001. [Хуторской, А. Современная дидактика. Санкт-Петербург, Москва, 2001]. [Online]. Available: <https://pps.kaznu.kz/ru/Main/FileShow/1901801/105/359/4130/%20%20%20%20%200/2024/1>. [Accessed January 22, 2026].
- [17] A. Januszewski and M. Molenda, eds., *Educational technology: A definition with commentary*. London, UK.: Routledge, 2013.
- [18] K. Heggart, A. Ritzhaupt, C. Prokes and R. Kimmons, "Educational Technology: Offering A Contemporary Definition," *The Journal of Applied Instructional Design*, vol. 14, no. 2, pp. 52–58, 2025. [Online]. Available: <https://edtechbooks.s3.us-west-2.amazonaws.com/pdfs/2222/21453.pdf>. [Accessed January 15, 2026].
- [19] D. Hlynka and M. Jacobsen, "What is educational technology, anyway? A commentary on the new AECT definition of the field," 2009. [Online]. Available: <https://ucalgary.scholaris.ca/server/api/core/bitstreams/b447ec3b-a79d-48a0-b7f8-9a5525f56d62/content>. [Accessed January 16, 2026].
- [20] M. D. Todino, "Educational Technologies." *Encyclopedia*, 2025. [Online]. Available: https://www.researchgate.net/profile/Michele-Todino/publication/388949036_Educational_Technologies/links/67add745207c0c20fa85d434/Educational-Technologies.pdf. [Accessed January 16, 2026].
- [21] P. Wang, "On defining artificial intelligence," *Journal of artificial general intelligence*, vol. 10, no. 2, pp. 1–37, 2019. [Online]. [Accessed January 16, 2026], <https://doi.org/10.2478/jagi-2019-0002>.
- [22] H. Sheikh, C. Prins and E. Schrijvers, "Artificial intelligence: definition and background," in *Mission AI: The new system technology*. Cham: Switzerland: Springer International Publishing, 2023, pp. 15–41. [Online]. Available: Springer Nature Link, https://link.springer.com/chapter/10.1007/978-3-031-21448-6_2?trk=public_post_comment-text [Accessed January 17, 2026], https://doi.org/10.1007/978-3-031-21448-6_2.
- [23] H. Abbass, "What is artificial intelligence?," *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 94–95, 2021. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=9523786>. [Accessed January 17, 2026].

- [24] High-Level Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines," Brussels, Belgium, 2018. [Online]. Available: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf. [Accessed January 19, 2026]
- [25] S. N. Akinwalere and V. Ivanov, "Artificial intelligence in higher education: Challenges and opportunities," *Border Crossing*, vol. 12, no. 1, p. 1, 2022. [Online]. Available: CEEOL, <https://www.ceeol.com/Search/Article-Detail?Id=1059714>. [Accessed January 19, 2026], DOI: <https://doi.org/10.33182/bc.v12i1.2015>.
- [26] M. O. Hagler and W. M. Marcy, "The legacy of PLATO and TICCIT for learning with computers," *Computer Applications in Engineering Education*, vol. 8, no. 2, pp. 127-131, 2000. [Abstract] Available: Wiley Online Library, [https://onlinelibrary.wiley.com/doi/abs/10.1002/1099-0542\(2000\)8:2%3C127::AID-CAE7%3E3.0.CO;2-H](https://onlinelibrary.wiley.com/doi/abs/10.1002/1099-0542(2000)8:2%3C127::AID-CAE7%3E3.0.CO;2-H). [Accessed January 16, 2026], DOI: [10.1002/1099-0542\(2000\)8:2%3C127::AID-CAE7%3E3.0.CO;2-H](https://doi.org/10.1002/1099-0542(2000)8:2%3C127::AID-CAE7%3E3.0.CO;2-H).
- [27] J. Huang, S. Salmiza and Y. Liu, "A review on artificial intelligence in education," *Academic Journal of Interdisciplinary Studies*, vol. 10, no. 3, 2021. [Online]. Available: <https://pdfs.semanticscholar.org/4590/d37ca3f650e9f72613189003a8c49eddb75b.pdf>. [Accessed January 19, 2026], DOI: <https://doi.org/10.36941/ajis-2021-0077>.
- [28] E. Vázquez-Cano, "Artificial intelligence and education: A pedagogical challenge for the 21st century," *Educational Process: International Journal (EDUPIJ)*, vol. 10, no. 3, pp. 7-12, 2021. [Online]. Available: https://www.edupij.com/files/1/articles/article_225/EDUPIJ_225_article_60ee3ea7423ed.pdf. [Accessed January 19, 2026].
- [29] E. Igbaseimokumo, "Historical development of artificial intelligence in education: The challenges and prospects," *Port Harcourt Journal of Educational Studies (PHAJOES), Conference Edition*, vol. 10, no. 1, Jan. 2025. [Online]. Available: <https://phajournal-unipor.org/wp-content/uploads/2025/09/1.HISTORICAL-DEVELOPMENT-OF-ARTIFICIAL-INTELLIGENCE-IN-EDUCATION-THE-CHALLENGES-AND-PROSPECTS-Elizabeth-Igbaseimokumo.pdf>. [Accessed January 20, 2026].
- [30] M. Baig, E. Yadegaridehkordi, "ChatGPT in the higher education: A systematic literature review and research challenges," *International journal of educational research*, vol. 127, 102411, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0883035524000971>. [Accessed May 13, 2026].
- [31] B. Ogunleye et al., "A systematic review of generative AI for teaching and learning practice," *Education Sciences*, vol., no 6, 2024. [Online]. Available: <https://www.mdpi.com/2227-7102/14/6/636>. [Accessed May 13, 2026].
- [32] Y. Albadari, et al., "A systematic literature review of empirical research on ChatGPT in education," *Discover Education*, vol. 3, no 60, 2024. [Online]. Available: <https://link.springer.com/article/10.1007/s44217-024-00138-2>. [Accessed May 13, 2026].
- [33] F. MO et al., "Undergraduate students' learning outcomes with ChatGPT: A meta-analytic study," *Computers and Education: Artificial Intelligence*, vol. 10, 100536, 2026. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2666920X25001766>. [Accessed May 13, 2026].
- [34] S. Gill et al., "Transformative effects of ChatGPT on modern education: Emerging Era of AI Chatbots," *Internet of Things and Cyber-Physical Systems*, vol. 4, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2667345223000354>. [Accessed May 13, 2026].
- [35] X. Song et al., "Integrating AI in college education: positive yet mixed experiences with ChatGPT," *Meta-Radiology*, vol. 2, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2950162824000675>. [Accessed May 13, 2026].
- [36] J. Báez, Bjugstad, A., Park, T. K., Jones, J. L., Bidwell, L. N., Sage, M., & Hitchcock, "Social work educators innovating with generative AI: An exploratory study," *Journal of Social Work Education*, vol. 61, no. 1, pp. 14-29, 2025. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/10437797.2024.2411170>. [Accessed May 13, 2026].
- [37] B. Meinhardt-Injac, J. Späte, L. Siemer & S. Witter, "Acceptance of ChatGPT in social work students," *In Forum for Education Studies*, Academic Publishing. vol. 3, no.1, 2025. [Online]. Available: https://www.researchgate.net/publication/389981829_Acceptance_of_ChartGPT_in_social_work_students. [Accessed May 13, 2026].
- [38] M. Segal, "Social workers' evaluation of ChatGPT for solving ethical dilemmas within the limits of confidentiality," *Journal of Social Work Practice*, vol. 40, no. 1, pp. 5-18, 2026. [Online]. Available: <https://www.tandfonline.com/doi/full/10.1080/02650533.2025.2480092>. [Accessed May 13, 2026].
- [39] A. Al-Zahrani, "Exploring the impact of artificial intelligence chatbots on human connection and emotional support among higher education students," *Sage Open*, vol. 15, no. 2, 2025. [Online]. Available: <https://journals.sagepub.com/doi/full/10.1177/21582440251340615>. [Accessed May 13, 2026].

Application of Fuzzy Logic in the Prediction of Air Pollution in Berlin, Germany

Desislava Velinova

Development of CAI System

Bulgarian Defence Institute

“Prof. Tsvetan Lazarov”

Sofia, Bulgaria

velinova.desislava@gmail.com

Abstract— Air pollution is the presence of harmful substances in the atmosphere that can adversely impact human health and other living organisms. In urban environments such as Berlin, air pollution—particularly from traffic emissions and industrial activities—continues to be a significant concern. The Air Quality Index (AQI) is commonly used to represent the level of air quality in a given area, based on the average concentrations of pollutants including particulate matter (PM₁₀ and PM_{2.5}), ozone (O₃), carbon dioxide (CO₂), sulphur dioxide (SO₂), and nitrogen dioxide (NO₂). Accurate prediction of AQI values is crucial for mitigating the negative effects of air pollution on both the environment and public health. This paper proposes a model for AQI prediction using a fuzzy data. By applying fuzzy sets and fuzzy logic techniques, an approach is presented to handle inaccurate, incomplete, or subjective data, to achieve more reliable and robust air quality assessments.

Keywords— Air pollution, Air quality index (AQI), Fuzzy Inference System (FIS), Fuzzy Logic

I. INTRODUCTION

In recent years, the development of industry and transportation has improved human life, but it has also led to increased environmental pollution, especially air pollution. Air pollution is defined as presence of harmful substances in the atmosphere that adversely affect human health, ecosystems, and even the climate. It arises from both human-related activities – such as transportation emissions, industry, energy production, burning fossil fuels, agricultural practices, and waste burning - and natural sources, including wildfires, volcanic activity, dust storms, and pollen. Some of the most important pollutants include:

- Particulate matter (PM₁₀ and PM_{2.5}): tiny particles that can enter the lungs and bloodstream

- Ozone (O₃): a gas that forms when pollutants react in sunlight
- Nitrogen dioxide (NO₂): mainly from traffic and industry
- Sulfur dioxide (SO₂): from burning coal and oil
- Carbon monoxide (CO): from incomplete combustion (e.g., car engines)

Air pollution remains the most significant environmental risk factor for health in Europe. Air pollutants such as particulate matter (PM₁₀ and PM_{2.5}), nitrogen dioxide (NO₂), and ozone (O₃) can lead to respiratory diseases (like asthma and bronchitis), cardiovascular diseases, type 2 diabetes, neurodegenerative diseases (e.g., dementia), and cancer. Fine particulate matter (PM_{2.5}) is especially dangerous because they can penetrate deep into the lungs and even enter the bloodstream. Sulfur dioxide (SO₂) irritates mucous membranes and can cause eye irritation and respiratory problems. Despite EU limits, pollution levels are often exceeded, making PM_{2.5} a growing global concern.

Air pollution doesn't just affect humans. It contributes to climate change, causes acid rain, damaging forests and lakes, harms wildfires and crops, reduces visibility (smog).

Predicting pollution levels and taking preventive measures—such as traffic restrictions and health warnings—are key to protecting public health. Urban areas are particularly affected due to industry and traffic, while weather conditions can influence how pollution spreads, sometimes carrying it across regions. Because of this, monitoring and coordinated global action are essential.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.96>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Advances in scientific research on the causes of air pollution and the development of mitigation strategies are essential for implementing effective control measures, forecasting pollution levels, and providing timely warnings to vulnerable populations when hazardous air quality conditions arise. This paper presents a model for predicting the Air Quality Index (AQI) using a proposed Fuzzy Inference System (FIS) model. A Mamdani-based FIS was developed to evaluate AQI by considering five major input pollutants: PM₁₀, PM_{2.5}, NO₂, O₃ and SO₂. The second section describes the data collection process and the employed methodology. The third section presents the analysis of the results, discusses model improvements, and the key research findings.

II. DATA AND METHODOLOGY

Data Collection

Hourly data on particulate matter (PM₁₀ and PM_{2.5}), nitrogen dioxide (NO₂), ozone (O₃), and carbon monoxide (CO) is collected from the monitoring station located in an urban area on Frankfurter Allee in Berlin. A total of 2160 data sets are collected from 1st January to 31st March 2026. They were obtained from the Federal Environment Agency in Germany. In this article was used only one week a hourly data set

Air quality index (AQI) Rating Scale

In Europe, air quality is monitored to protect health in accordance with the EU Ambient Air Quality Guideline (AAQD). The new European Air Quality Directive 2024/2881 introduces stricter limit values for air pollutants, which will become binding in the member states from 2030 [1].

The rating scale of the AQI status indicator consists pollutant concentrations, that are classified into five index categories from "very good" to "very poor" using threshold values as shown in Table 1. It is based on hourly average measurements of ozone (O₃), nitrogen dioxide (NO₂), particulate matter (PM₁₀ and PM_{2.5}), and sulfur dioxide (SO₂). The values are hourly averages measured in micrograms per cubic meter (µg/m³). This measurement is based on classification made from the Federal Environment Agency in Germany [1]. These threshold values were derived based on current health studies and taking into account the recommendations of the World Health Organization (WHO) [8].

TABLE 1 AIR QUALITY INDEX (AQI) [1]

Air Quality Index (AQI)	PM ₁₀	PM _{2.5}	O ₃ (Ozone)	NO ₂	SO ₂
Very poor	over 90	over 50	over 240	over 100	over 100
Poor	55–90	31–50	145–240	61–100	61–100
Moderate	28–54	16–30	73–144	31–60	31–60
Good	10–27	6–15	25–72	11–30	11–30

Air Quality Index (AQI)	PM ₁₀	PM _{2.5}	O ₃ (Ozone)	NO ₂	SO ₂
Very Good	0–9	0–5	0–24	0–10	0–10

Data Analysis

Data analysis was performed using MATLAB, a powerful software platform equipped with numerous built-in tools for problem-solving and graphical visualization. A fuzzy inference system is a principled control system based on the fuzzy theory. The method used to predict the Air Quality Index (AQI) through a Fuzzy Inference System (FIS) consists of four main steps: (I) Fuzzification of input and output variables, (II) Fuzzy Inference, which involves selecting appropriate membership functions for both input and output variables, (III) the development of a fuzzy rule base, which defines the application of logical rules, and (IV) Defuzzification, where fuzzy results are converted into a crisp output value [6]. The overall structure of the fuzzy system is illustrated in Figure 1 [3].

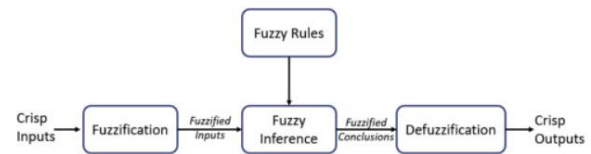


Fig. 1. Fuzzy Inference System [3]

I) Fuzzification of input and output variables

Fuzzification is the process of transforming crisp numerical values into fuzzy values. In this step, real or measured input data are interpreted as linguistic variables using appropriate membership functions. These functions represent human reasoning and uncertainty by assigning degrees of membership to each input. Both input and output variables are expressed in linguistic terms such as "Very Good," "Good," "Moderate," "Poor," and "Very Poor."

First, it was selected the system variables. The most important input variables are PM₁₀, PM_{2.5}, O₃, NO₂ and SO₂. As the number of input variables in the system increases, a larger number of fuzzy rules is required to describe all possible input–output relationships. Consequently, the complexity of the system increases significantly. The input and output are taken in the form of linguistic format. For example, PM₁₀ = (Very Good, Good, Moderate, Poor, Very Poor), PM_{2.5} = (Very Good, Good, Moderate, Poor, Very Poor), O₃ = (Very Good, Good, Moderate, Poor, Very Poor), NO₂ = (Very Good, Good, Moderate, Poor, Very Poor), SO₂ = (Very Good, Good, Moderate, Poor, Very Poor). The output variable AQI = (Good, Moderate, Unhealthy for Sensitive Groups, Unhealthy, Very Unhealthy).

Figure 2 shows the fuzzy inference system that consists of five inputs (PM₁₀, PM_{2.5}, O₃, NO₂ and SO₂) and one output which is air quality index (AQI). By using FIS editor and membership function editor from MATLAB software all the membership functions are developed.

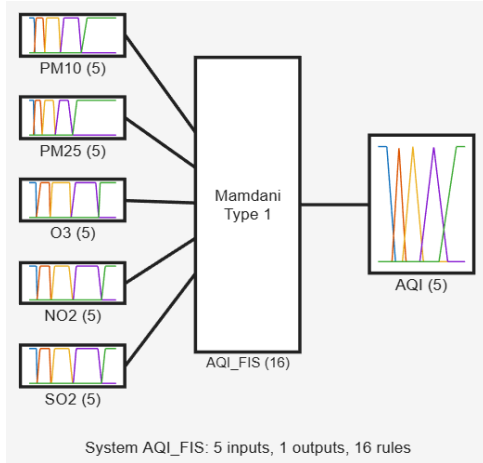


Fig. 2. AQI Determination Using Fuzzy Logic

II) Fuzzy Inference – Selection of Membership Functions for Input and Output Variables

Linguistic values are represented using fuzzy sets. Each fuzzy set is characterized by a membership function that defines the degree of belonging of an element to the set. Triangular and trapezoidal membership functions are commonly used due to their simplicity and computational efficiency. In this article, it was used trapezoidal function. Mathematically, the trapezoidal membership function is defined as follows:

$$\mu_{\text{triangle}}(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a \leq x \leq b \\ 1, & b \leq x \leq c \\ \frac{d-x}{d-c}, & c \leq x \leq d \\ 0, & d \leq x \end{cases} \quad (1)$$

The trapezoidal membership function, shown in Equation 1, is defined by a lower limit a , an upper limit d , a lower support limit b , and an upper support limit c , where $a < b < c < d$.

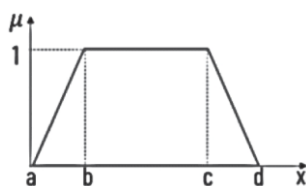


Fig. 3. Trapezoidal membership function [5]

This function is used to map linguistic values into the range $[0, 1]$, representing the degree of membership in the fuzzy set. The membership function of input and output are represented in Figure 4 and Figure 5.

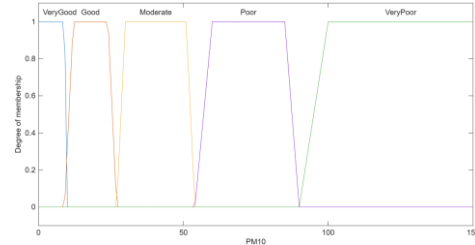


Fig. 4(a). Membership function of PM₁₀

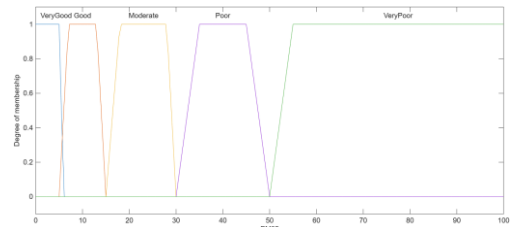


Fig. 4(b). Membership function of PM_{2.5}

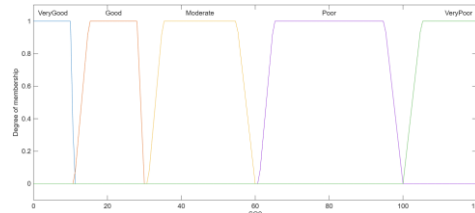


Fig. 4(c). Membership function of SO₂

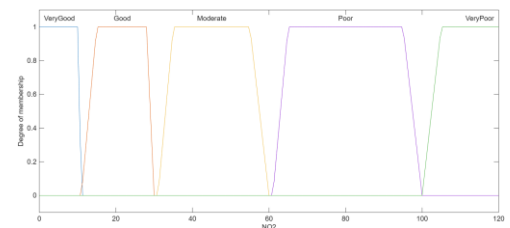


Fig. 4(d). Membership function of NO₂

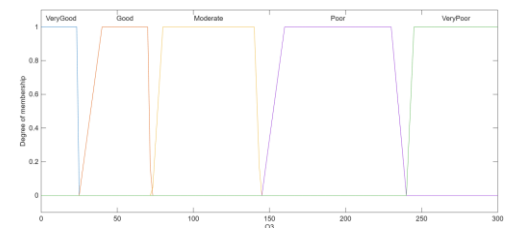


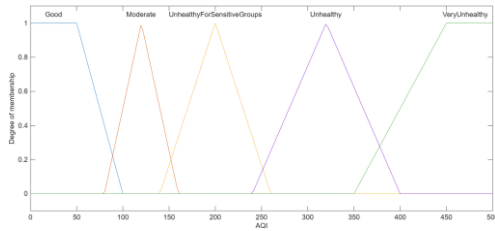
Fig. 4(c). Membership function of O₃

Fig. 5. Membership function of output AQI

Table 2 presents the trapezoidal membership function parameters for each input variable (PM₁₀, PM_{2.5}, O₃, NO₂, SO₂), while Table 3 shows the corresponding parameters for the output variable (AQI). These parameters define the fuzzy sets used in the FIS for air quality evaluation.

TABLE 2 PARAMETERS FOR MEMBERSHIP FUNCTION OF THE INPUTS

AQI Category	PM ₁₀ [a b c d]	PM _{2.5} [a b c d]	O ₃ [a b c d]	NO ₂ [a b c d]	SO ₂ [a b c d]
Very Good	[0 0 9 10]	[0 0 5 6]	[0 0 24 25]	[0 0 10 11]	[0 0 10 11]
Good	[9 12 24 27]	[5 7 13 15]	[25 40 70 72]	[11 15 28 30]	[11 15 28 30]
Moderate	[27 30 51 54]	[15 18 28 30]	[73 80 140 144]	[31 35 55 60]	[31 35 55 60]
Poor	[54 60 85 90]	[30 35 45 50]	[145 160 230 240]	[61 65 95 100]	[61 65 95 100]
Very Poor	[90 100 150 150]	[50 55 100 100]	[240 245 300 300]	[100 105 120 120]	[100 105 120 120]

TABLE 3 PARAMETERS FOR MEMBERSHIP FUNCTION OF THE OUTPUT

AQI Category	AQI [a b c d]
Very Good	[0 0 50 100]
Good	[50 100 100 150]
Moderate	[150 150 200 250]
Poor	[250 250 300 350]
Very Poor	[350 400 500 500]

III) Fuzzy Rules

The rules determine how the membership functions of the inputs and output are used in the fuzzy inference process. These rules are linguistic in nature and are expressed as “IF–THEN” statements. The proposed fuzzy model is based on the Mamdani fuzzy inference structure, as described in Equation 2 [4].

$$R_i: \text{IF } X_1 \text{ is } L_1 \wedge X_2 \text{ is } L_2 \wedge X_3, \dots \text{is } L_{M-1} \wedge X_M \text{ is } L_M \text{ THEN } \mu_{iR} \rightarrow Y \quad (2)$$

Where $i: 1, \dots, n$

$L' \in \{L_{jk}\} j: 1, \dots, m; k: 1, \dots, n$; n : the number of linguistic labels defined for the j input variables; R_i is the i -th rule in the set of fuzzy rules; X_M is L'_M states that the fuzzy input variable X_M has a certain linguistic value in L' ; $\mu_{iR} \rightarrow Y$ implies that the degree of membership μ in the rules dictates the consequent fuzzy set Y .

Figure 6 shows the table with rules in that is set up in the rule editor in MATLAB software. There are generated 16 rules used to evaluate the AQI by using Mamdani IF–THEN rules to determine whether it is good, moderate, unhealthy for the sensitive groups, unhealthy and very unhealthy. The rules below show an example of IF–THEN rules of AQI implemented in the MATLAB software.

	Rule	Weight	Name
1	If PM10 is VeryGood and PM25 is VeryGood and O3 is VeryGood and NO2 is VeryGood and SO2 is VeryGood then AQI is VeryGood	1	rule1
2	If PM10 is Good and PM25 is Good and O3 is Good and NO2 is Good and SO2 is Good then AQI is Good	1	rule2
3	If PM25 is Good and NO2 is Good then AQI is Moderate	1	rule3
4	If PM25 is Moderate and NO2 is Moderate then AQI is UnhealthyForSensitiveGroups	1	rule4
5	If O3 is Moderate then AQI is UnhealthyForSensitiveGroups	1	rule5
6	If PM10 is Moderate and SO2 is Moderate then AQI is UnhealthyForSensitiveGroups	1	rule6
7	If PM25 is Poor then AQI is Unhealthy	1	rule7
8	If PM25 is VeryPoor then AQI is VeryUnhealthy	1	rule8
9	If PM10 is Poor and NO2 is Moderate then AQI is Unhealthy	1	rule9
10	If PM10 is VeryPoor then AQI is VeryUnhealthy	1	rule10
11	If NO2 is Poor then AQI is Unhealthy	1	rule11
12	If NO2 is VeryPoor then AQI is VeryUnhealthy	1	rule12
13	If SO2 is Poor then AQI is Unhealthy	1	rule13
14	If SO2 is VeryPoor then AQI is VeryUnhealthy	1	rule14
15	If O3 is Poor then AQI is Unhealthy	1	rule15
16	If O3 is VeryPoor then AQI is VeryUnhealthy	1	rule16

Fig. 6. The rule base coded using MATLAB software

IV) Defuzzification

Defuzzification is the process of converting fuzzy values into crisp outputs. In this study, the centroid method is applied, which is one of the most commonly used techniques for defuzzification. Using this approach, the fuzzy number is geometrically determined to produce a single crisp value [4].

After defining the rules, the data has been inserted in the Rule Viewer and the result is generated as shown in the right-end column of Figure 7. The figure visualizes how input variables are processed through a Mamdani-type Fuzzy Inference System to produce an output value for the AQI.

On the left side, are displayed the input variables PM₁₀, PM_{2.5}, O₃, NO₂, and SO₂. Each input has a numerical value at the top for every input value (e.g., PM₁₀ = 75, PM_{2.5} = 50, etc.) and a set of horizontal bars representing their membership in different fuzzy sets (such as low, moderate, or high). The coloured regions indicate the degree to which each input belongs to a particular fuzzy category.

Each row corresponds to a fuzzy rule, and the system includes 16 rules in total. These rules combine the input conditions using fuzzy logic to determine their contribution to the output.

On the right side, the output variable AQI is shown. The triangular shapes represent the output membership functions, and the highlighted areas indicate the aggregated result after applying all active rules. The final crisp AQI value (e.g., AQI = 320) is obtained through a defuzzification process.

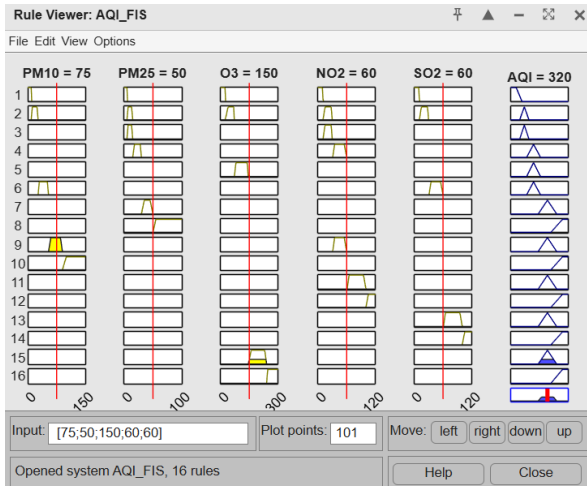


Fig. 7. Rule Viewer (Rules 1-16)

Figure 8 presents a 3D-surface plot illustrating the relationship between particulate matter concentrations and the proposed from FIS AQI. The two horizontal axes represent input air pollutants - PM₁₀ and PM_{2.5}, while the vertical axis represents the output variable - AQI. The surface shows how variations in particulate matter levels influence the predicted air quality. The colour - from dark blue to yellow - indicates increasing AQI values. Lower AQI values are shown in darker blue regions, while higher values transition through green and orange to yellow, representing poorer air quality conditions. The surface is mostly flat at lower pollution levels, suggesting relatively stable and lower AQI values.

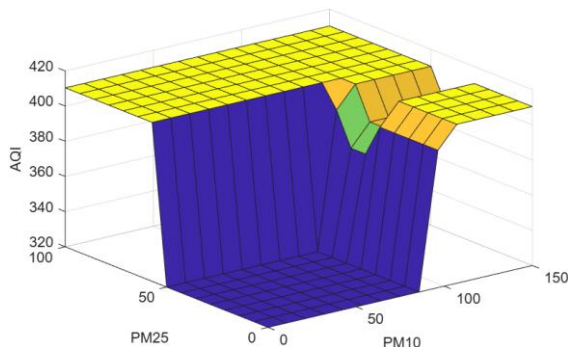


Fig. 8. Surface view of the particulate matter in FIS

III. FINDINGS AND DISCUSSION

The proposed model consists of several sequential steps for predicting and evaluating the AQI using fuzzy logic. First, hourly air quality and environmental data are collected from monitoring station, such as those located in Berlin. The input parameters include major air pollutants such as PM_{2.5}, PM₁₀, NO₂, SO₂, and O₃, while the output variable is the AQI.

Next, appropriate ranges are defined for each pollutant concentration and AQI level. The pollutant concentrations are categorized into linguistic terms such as Very Good, Good, Moderate, Poor, and Very Poor. Similarly, AQI values are classified into categories including Good, Moderate, Unhealthy for Sensitive Groups, Unhealthy, and Very Unhealthy.

In the fuzzification stage, the crisp numerical pollutant values are converted into fuzzy linguistic variables. Membership functions, typically triangular or trapezoidal in shape, are defined to represent the degree of belonging of each input value to a specific linguistic category.

After fuzzification, a rule base is developed using expert knowledge and environmental standards. These IF-THEN rules establish relationships between pollutant levels and the corresponding AQI category.

The fuzzy inference process is then carried out using a FIS. Commonly used methods include the Mamdani Fuzzy Inference System, which is interpretable and rule-based, and the Sugeno Fuzzy Model, which is more suitable for optimization and computational efficiency. In this study, the Mamdani Fuzzy Inference System is adopted because of its simplicity and interpretability in AQI prediction.

Following inference, defuzzification is performed to convert the fuzzy output into a single crisp AQI value. Several methods can be applied, including the centroid method and the mean of maxima method. In this work, the centroid method is used due to its wide acceptance and effectiveness.

Finally, the output AQI values obtained from the fuzzy model are evaluated by comparing the predicted AQI values with the actual AQI measurements. This comparison helps assess the accuracy and overall performance of the proposed fuzzy logic model.

Table 4 presents a small set of real air quality data along with a comparison between the FIS-predicted AQI and the actual measured AQI. The air quality data used in this study are obtained from a monitoring station located in Berlin (Frankfurter Allee). The dataset includes hourly measurements of the following pollutants: PM₁₀, PM_{2.5}, NO₂, and O₃. However, it is important to note that SO₂ (sulfur dioxide) measurements are not available from this station. Despite this limitation, the developed fuzzy inference system (FIS) includes SO₂ as one of its input variables. To address this issue, a constant value of zero

(SO₂ = 0) was used as a placeholder during the AQI prediction process.

TABLE 4 RESULT OF COMPARISON BETWEEN ACTUAL AQI AND FIS OUTPUT

Date Time	PM ₁₀	PM _{2.5}	NO ₂	O ₃	SO ₂	FIS AQI	Actual AQI
01.03.2026 00:00	22	10	20	56	0	68.66	54.267
01.03.2026 01:00	16	7	14	66	0	74.98	86.933
01.03.2026 02:00	20	6	10	70	0	88.54	100
01.03.2026 03:00	14	6	17	62	0	61.45	73.867
01.03.2026 04:00	12	7	13	62	0	65.33	73.867
01.03.2026 05:00	13	8	10	65	0	74.76	83.667
01.03.2026 06:00	11	6	10	69	0	105.45	96.733
01.03.2026 07:00	9	6	15	64	0	75.16	80.4
01.03.2026 08:00	13	6	16	65	0	76.12	83.667
01.03.2026 09:00	25	8	17	66	0	81.99	86.933
01.03.2026 10:00	23	9	15	63	0	82.76	83.667
01.03.2026 11:00	21	10	16	61	0	81.54	84.863
01.03.2026 12:00	22	9	15	64	0	80.76	84.377

The results presented in this study are based on one week of hourly measurements. The developed fuzzy inference system is based on a relatively small rule base consisting of 16 rules. While this limited number of rules is sufficient to capture the general behavior of air quality and provides reasonably accurate AQI predictions, it does not fully represent all possible combinations of pollutant conditions. As a result, some deviations between the FIS-predicted AQI and the actual AQI were observed.

Table 5 shows the comparison between linguistic values of the FIS output and the actual AQI values from Table 4. Most of the predicted AQI values were classified as *Moderate*, which matched the actual AQI classifications. The results show that the system performed well in predicting the correct air quality category. Out of the thirteen observations, twelve were correctly classified by the FIS. Only one value showed a mismatch, where the FIS predicted an AQI of 105.45 and classified it as *Unhealthy for Sensitive Groups*, while the actual AQI value was 96.733 and belonged to the *Moderate* category. This difference occurred because the predicted value slightly exceeded the threshold value of 100, which separates the two linguistic categories. Overall, the results indicate that the FIS provides reliable AQI classification and effectively handles gradual transitions between air quality categories through fuzzy logic reasoning.

TABLE 5 RESULT OF COMPARISON BETWEEN LINGUISTIC VALUE OF ACTUAL AQI AND FIS OUTPUT

FIS AQI	Linguistic Value	Actual AQI	Linguistic Value
68.66	Moderate	54.267	Moderate
74.98	Moderate	86.933	Moderate
88.54	Moderate	100	Moderate
61.45	Moderate	73.867	Moderate
65.33	Moderate	73.867	Moderate
74.76	Moderate	83.667	Moderate
105.45	Unhealthy for Sensitive Groups	96.733	Moderate
75.16	Moderate	80.4	Moderate
76.12	Moderate	83.667	Moderate
81.99	Moderate	86.933	Moderate
82.76	Moderate	83.667	Moderate
81.54	Moderate	84.863	Moderate
80.76	Moderate	84.377	Moderate

The comparison results indicate the overall performance of the model. From the total data based on one week and collected within 168 hours, there are 149 TRUE statements and 18 FALSE statements. The level of accuracy rate is calculated as follows:

$$\text{Accuracy Rate} = \frac{149}{168} \times 100 = 88,69\%$$

However, the model performance can be further improved by incorporating a larger and more diverse dataset. To improve the accuracy and robustness of the model, the rule base can be expanded by adding more fuzzy rules. A larger and more detailed rule set would allow the system to better handle different pollutant interactions and provide smoother and more precise AQI predictions.

The results of comparison between the actual AQI values and the FIS-predicted AQI demonstrates that the fuzzy inference system provides a good approximation of real air quality conditions. Furthermore, the FIS output follows the same trend as the actual AQI, although slight overestimations and underestimations were observed. These can be reduced by incorporating more extensive datasets and refining the fuzzy rule base.

IV. CONCLUSION

The main objective of this study was to accurately predict the Air Quality Index (AQI) using a proposed Fuzzy Inference System (FIS) model. A Mamdani-based

FIS was developed to evaluate AQI by considering five major input pollutants: PM₁₀, PM_{2.5}, NO₂, O₃ and SO₂. The evaluation process follows four key steps: fuzzification, fuzzy inference, application of fuzzy rules, and defuzzification. The model demonstrated a good accuracy rate, indicating that the proposed Mamdani FIS effectively predicts AQI and provides a reliable tool for assessing air quality; however, the model can be extended and improved by expanding the fuzzy rule base and incorporating more extensive and diverse datasets.

ACKNOWLEDGEMENTS

This work was supported by the NSP “Security and defence” program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

- [1] Umweltbundesamt, “Der Luftqualitätsindex - LQI”. [Online]. Available: <https://www.umweltbundesamt.de/themen/luft/luftqualitaet/der-luftqualitaetsindex-lqi#der-luftqualitaetsindex-lqi-des-umweltbundesamtes> [Accessed: April. 01, 2026].
- [2] Berliner Luftgütemessnetz Stationsdaten: 174 Frankfurter Allee. [Online]. Available: <https://luftdaten.berlin.de/station/mc174> [Accessed: April. 01, 2026].
- [3] Science Direct, “Fuzzy Inference System”. [Online]. Available: <https://www.sciencedirect.com/topics/engineering/fuzzy-inference-system> [Accessed: April. 01, 2026].
- [4] N.Shafii, N. Ramle, R.Alias, D.Nasir, “Application of Fuzzy Inference System in the Prediction of Air Quality Index”, September 2021. ”. [Online]. Available: https://www.researchgate.net/publication/354871675_Application_of_Fuzzy_Inference_System_in_the_Prediction_of_Air_Quality_Index [Accessed: April. 01, 2026].
- [5] Codecrucks, “What is fuzzy membership function - a complete guide”, 2021. [Online]. Available: <https://codecrucks.com/what-is-fuzzy-membership-function-complete-guide/> [Accessed: Mai. 05, 2026].
- [6] S.Himanshu, Y.A.Lone, “Deep Neuro-Fuzzy Systems with Python”, Apress, December 2019
- [7] R.Saatchi, “Fuzzy Logic Concepts, Developments and Implementation”, October 2024. [Online]. Available: <https://www.mdpi.com/2078-2489/15/10/656> [Accessed: April. 01, 2026].
- [8] World Health Organisation. [Online]. Available: <https://www.who.int/tools/air-quality-standards> [Accessed: April.08,2026]
- [9] Z.Zulkiflee, A. Idris, “Fuzzy Inference System Model for Air Quality Index Prediction” 2024. [Online]. Available: <https://science.utm.my/proccsimath/wp-content/uploads/sites/605/2024/09/133-143-ZULFAZLEEN-NATASHA-BINTI-ZULKIFLEE-A20SC0435.pdf> [Accessed: April. 08, 2026].
- [10] H. Liu., Q. Li, D. Yu., & Y. Gu.: Air quality index and air pollutant concentration prediction based on machine learning algorithms, 2019, Applied Sciences (Switzerland). [Online]. Available: <https://doi.org/10.3390/app9194069> [Accessed: April. 08, 2026].
- [11] R. Kumaravel, V. Vallinayagam.: A Fuzzy Inference System for air quality in using Matlab, Chennai, India. In J. Environ. Res. Develop. Journal of Environmental Research And Development (Vol. 7, Issue 1).
- [12] Matlab Hilfe Center, “Mamdani and Sugeno Fuzzy Inference Logic”. [Online]. Available: <https://de.mathworks.com/help/fuzzy/types-of-fuzzy-inference-systems.html> [Accessed: April. 08, 2026].
- [13] H.Herpratiwi, M.Maftuh, W.Firdaus, A.Tohir, M.Daulay, R.Rahim, “Implementation and Analysis of Fuzzy Mamdani Logic Algorithm from Digital Platform and Electronic Resource”, August 2022. [Online]. Available: https://www.researchgate.net/publication/363144501_Implementation_and_Analysis_of_Fuzzy_Mamdani_Logic_Algorithm_from_Digital_Platform_and_Electronic_Resource [Accessed: April. 08, 2026].
- [14] K.Pujaru, S.Adak, T.K.Kar, S.Patra, S.Jana, “A Mamdani fuzzy inference system with trapezoidal membership functions for investigation fishery production”, May 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2772662224000857> [Accessed: April. 08, 2026].
- [15] D.Dunea, A.A.Pohoata, E.Lungru, “Fuzzy inference system for estimation of air quality index”. [Online]. Available: <https://rj.romai.ro/arhiva/2011/2/Dunea-et-al.pdf> [Accessed: April. 08, 2026].
- [16] IQAir, “Air quality in Berlin”. [Online]. Available: <https://www.iqair.com/germany/berlin/berlin> [Accessed: April. 05, 2026].
- [17] Matlab Hilfe-Center, “Fuzzy Inference System Modeling”. [Online]. Available: <https://de.mathworks.com/help/fuzzy/fuzzy-inference-system-modeling.html> [Accessed: April. 05, 2026].
- [18] M.Saleem, N.Shingari, M.Farooq, B.Mago, M.Khan, “Real-Time Air Quality Monitoring Model using Fuzzy Inference System”, 2024. [Online]. Available: https://thesai.org/Downloads/Volume15No6/Paper_84-Real_Time_Air_Quality_Monitoring_Model.pdf [Accessed: April. 05, 2026].

Empirical Study of Incident Response Practices for Personal Data Breaches in Bulgarian Organizations

Martin Zahariev

Faculty of Information Sciences,
National Security Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
m.zahariev@unibit.bg

Daniela Pavlova

Faculty of Information Sciences,
Computer Sciences Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Panayot Gindev

Information Systems and
Technologies Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
p.gindev@unibit.bg

George Dimitrov

Faculty of Information Sciences,
Computer Sciences Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
g.g.dimitrov@unibit.bg

Vyara Savova

University of Library Studies and
Information Technologies
Sofia, Bulgaria
vyara.savova@yahoo.com

Radoslava Makshutova

Institute for the State and the Law
Bulgarian Academy of Sciences
Sofia, Bulgaria
r.makshutova@gmail.com

Abstract—This paper presents an empirical study of incident response practices related to personal data breaches in Bulgarian organizations. The study examines how organizations detect, assess, and manage incidents involving personal data in accordance with personal data protection requirements. The research is based on data collected through a survey conducted among organizations from different economic sectors in Bulgaria. The analysis focuses on the existence of internal incident response procedures, the level of organizational preparedness, and the awareness of obligations arising from personal data breach incidents. The results reveal differences among organizations in terms of organizational measures, staff training, and incident management practices. Based on the analysis, conclusions are drawn regarding the implementation of incident response procedures and the management of personal data breach incidents in an organizational environment.

Keywords—data protection, incident management, incident response, personal data breach.

I. INTRODUCTION

In the contemporary digital environment, organizations process and store substantial volumes of personal data as part of their operations. The use of information systems, electronic services, and various technological solutions enhances the capabilities for data exchange and processing, while simultaneously creating conditions for the occurrence of incidents related to personal data breaches.

Such incidents may result in unauthorized access, loss, disclosure, or misuse of information containing personal data.

Under these conditions, organizations are required to implement appropriate organizational and technical measures to prevent and manage such incidents. These measures include the development of internal incident response procedures, staff training, and the implementation of mechanisms for the detection and analysis of personal data breaches. The management of such incidents necessitates clearly defined processes for identification, assessment, and response in the event of a breach.

The present study aims to analyze incident response practices related to personal data breaches in Bulgarian organizations. The study is based on data collected through a survey and examines issues related to the existence of incident response procedures, organizational preparedness, and approaches to managing such situations. The obtained results make it possible to identify observed practices and to draw conclusions regarding how organizations approach the management of personal data incidents.

A. Literature Review

The primary legal framework governing the management and notification of personal data breaches in the European Union is Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), which defines the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.70>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

concept of a “personal data breach” and establishes the obligation to notify the supervisory authority within 72 hours where there is a risk to the rights and freedoms of natural persons, as well as the requirement to internally document all identified breaches [1]. The guidelines of the European Data Protection Board (EDPB) further complement this framework by specifying the criteria for determining risk and high risk, the content of notifications, and the point at which the controller is considered to have become aware of a breach [2]. In addition, example breach scenarios—such as ransomware attacks, data leaks, human error, and lost devices—are examined to support organizations in risk assessment and decision-making regarding notification to supervisory authorities and affected individuals [3]. Practical application of these requirements can also be observed in the guidance issued by national supervisory authorities, where the minimum elements of internal documentation and the possibility of phased information provision during notification are outlined [4].

Incident response is also considered an organizational and technological process encompassing preparation, detection, containment, recovery, and post-incident analysis of root causes. In this context, the incident management framework of the National Institute of Standards and Technology (NIST) conceptualizes incident response as part of broader cybersecurity risk management activities and emphasizes the need for clearly defined roles, coordination among involved teams, and established mechanisms for communication and accountability [5]. In parallel, studies by the European Union Agency for Cybersecurity (ENISA) indicate that data security breaches often result from both malicious actions and human error, while delayed detection and limited visibility into incidents hinder their containment and subsequent recovery [6]. These findings suggest that effective incident response requires a combination of technical monitoring mechanisms and organizational procedures for incident management and reporting.

The scientific literature in the field of incident management indicates that organizational practices can be structured into phases encompassing preparation, response, and subsequent process improvement in incident management [7]. Despite the existence of established models and recommended practices, a number of studies note that their implementation within organizational environments is often uneven and accompanied by practical challenges. In the Bulgarian context, examples of formalized internal procedures for managing personal data breaches can also be identified, introducing criteria for risk assessment, breach categorization, and internal reporting mechanisms [8]. Nevertheless, the extent to which organizations in Bulgaria maintain consistent processes that integrate technical incident response with risk assessment and notification decision-making in the event of personal data breaches remains an open question. This gap highlights the need for empirical research into organizational practices in this area.

From a comparative perspective, the 72-hour notification deadline is a common GDPR requirement, but the practical tools for submitting notifications vary among national supervisory authorities. The European Data Protection Board (EDPB) maintains a consolidated page with guidance on notifying data breaches to the competent data protection authority [9]. In Ireland, the Data Protection Commission (DPC) requires breach notifications to be submitted through a dedicated Breach Notification Form and asks controllers to identify cross-border breaches in the relevant part of the form [10]. In France, the Commission nationale de l'informatique et des libertés (CNIL) emphasizes internal documentation, notification to the supervisory authority within 72 hours where there is a risk, and communication to data subjects where the risk is high [11]. In Spain, the Agencia Española de Protección de Datos (AEPD) provides guidance on risk assessment and indicates that notification to the supervisory authority is required where a risk exists and must be made within 72 hours [12]. These examples show that the need for clear forms, guidance, and practical decision-support tools is not specific to Bulgaria, although the present findings indicate that this need is especially visible among Bulgarian organizations.

II. MATERIALS AND METHODS

The present study was conducted within the framework of a research initiative aimed at analyzing organizational practices in incident response related to personal data breaches.

To collect empirical data, a standardized survey method was employed. A structured questionnaire was used, comprising closed-ended, semi-closed, and a limited number of open-ended questions. The questions were designed to identify organizational practices regarding internal reporting, risk assessment, the existence of incident response procedures, the application of guidelines and methodological documents, as well as the perception and use of available tools for incident notification and management.

The study included 49 valid responses from representatives of various types of organizations. These comprised private for-profit organizations, public institutions, non-profit organizations, as well as external consultants acting on behalf of specific organizations. In terms of organizational size, micro, small, medium, and large enterprises were represented, including a significant proportion of organizations with more than 250 employees. This diversity allows for observations to be made both with regard to organizational type and the scale of operations.

The participants were reached through a purposive, non-probability dissemination of the questionnaire among professional groups and individuals involved in personal data protection, legal compliance, information security, and incident response. The target audience included Data Protection Officers, legal advisers, lawyers, consultants, information technology specialists, and other persons involved in data protection processes within organizations. Because the questionnaire was distributed through

professional contacts and could be further forwarded, the exact number of persons reached by the invitation cannot be determined. Therefore, a response rate was not calculated. The 49 valid responses are treated as a sufficient empirical basis for an exploratory analysis of observed practices, difficulties, and tendencies, but not as a nationally representative sample.

The questionnaire was designed for the purposes of the present exploratory study and was structured around several thematic groups. The first group included questions related to the general profile of the organization. The second group focused on the existence of internal rules, procedures, and mechanisms for responding to incidents involving personal data. The third group addressed awareness and application of guidelines, recommendations, and methodological documents. The fourth group examined practical aspects of notification, internal coordination, and the perceived applicability of available tools. The final section provided respondents with the opportunity to offer additional comments and recommendations.

The present paper examines the results of the survey conducted among Bulgarian specialists and representatives of organizations involved in personal data protection, with a focus on the preparedness of organizations in Bulgaria to respond to personal data breaches. A separate survey among foreign specialists from other European Union Member States is planned within the broader research work. At the time of preparing this manuscript, that survey had not been completed; therefore, its results are not included in the present analysis. Consequently, the comparative observations in this paper are limited to publicly available guidance and procedures of selected supervisory authorities.

Data processing was conducted using descriptive analysis based on the frequency distribution of responses and comparisons across different groups of respondents. The analysis was aimed at identifying recurring patterns in organizational practices, differences among categories of organizations, and areas where challenges, insufficient awareness of procedures, or a lack of clearly defined internal mechanisms are observed.

In addition to the frequency-based presentation of the results, basic statistical checks were carried out for selected survey indicators. Their purpose is to show which observed proportions are clearly high or low. These checks are complementary and should be interpreted cautiously due to the limited sample size.

III. RESULTS AND DISCUSSION

The conducted survey includes 49 valid responses from representatives of organizations with diverse profiles and scales of operation. The sample is predominantly composed of public organizations (49.0%) and private for-profit organizations (40.8%), while in terms of size, the largest share is represented by organizations with 250 or more employees (59.2%). This distribution allows for the examination of incident response practices in organizations where personal data processing is relatively well

institutionalized and presupposes the existence of internal rules, defined responsibilities, and a more structured management framework. The profile of the sample is summarized in Table 1.

TABLE I. SAMPLE PROFILE (N = 49)

Group	Category	n	%
Type of organization	Public organization	24	49.0
	Private for-profit organization	20	40.8
	Other profiles	5	10.2
Size of organization	250 or more employees	29	59.2
	50–249 employees	12	24.5
	Other sizes	8	16.3

At the level of formal organizational preparedness, the results indicate a relatively good degree of initial compliance with personal data protection requirements. The presence of a Data Protection Officer was reported in 69.4% of organizations, 65.3% indicated that they have a designated individual or team responsible for incident response, 93.9% stated that they are familiar with the definition of a personal data breach under the GDPR, and 83.7% correctly recognized that all scenarios listed in the survey may constitute such a breach. These findings suggest that baseline regulatory awareness is relatively high and that, in a significant proportion of organizations, the minimum structural prerequisites for incident response have already been established. At the same time, the mere existence of formal mechanisms is not sufficient to conclude that a uniformly high level of practical preparedness is in place.

A more detailed examination of organizational and technical measures reveals a more heterogeneous picture. The highest values are observed in the implementation of technical measures such as encryption, network security, and access control (87.8%), as well as in restricting access based on job roles (79.6%). Relatively strong results are also recorded in the clear classification of sensitive data (73.5%), employee training to recognize and report potential breaches (71.4%), maintenance of records of processing activities (67.3%), and the existence of a written incident response plan (63.3%). In contrast, the more operational elements of preparedness remain significantly less developed. Only 53.1% of organizations use a system for incident logging and tracking, 51.0% conduct regular cybersecurity testing, 46.9% have a system for monitoring access to sensitive data, 42.9% use Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS)-type solutions, and only 26.5% carry out simulations or training exercises based on breach scenarios. This disparity indicates that, in many organizations, documented compliance measures are in place, but far fewer have been translated into regularly tested and repeatable practical response mechanisms. The main indicators of formal and operational preparedness are summarized in Table 2.

TABLE II. MAIN INDICATORS OF FORMAL AND OPERATIONAL PREPAREDNESS

Indicator	n	%
Presence of a Data Protection Officer	34	69.4
Designated individual/team for incident response	32	65.3
Existence of a written incident response plan	31	63.3
Employee training to recognize and report breaches	35	71.4
Implementation of appropriate technical security measures	43	87.8
Access restriction based on job roles	39	79.6
Incident logging and tracking system	26	53.1
Regular cybersecurity testing	25	51.0
Monitoring of access to sensitive data	23	46.9
Use of SIEM/IDS-type solutions	21	42.9
Simulations/training exercises	13	26.5

The results of the basic statistical checks are presented in Table 3.

TABLE III. BASIC STATISTICAL CHECKS FOR SELECTED INDICATORS

Indicator	Result
GDPR breach definition	46/49 (93.9%) CI 83.5-97.9 p<0.001
Technical security measures	43/49 (87.8%) CI 75.8-94.3 p<0.001
72-hour deadline awareness	35/49 (71.4%) CI 57.6-82.2 p=0.004
Simulations/training exercises	13/49 (26.5%) CI 16.2-40.3 p=0.001
Use of Guidelines 9/2022	7/49 (14.3%) CI 7.1-26.7 p<0.001
Notification of data subjects	4/49 (8.2%) CI 3.2-19.2 p<0.001

Note: CI denotes a 95% confidence interval calculated using the Wilson score method. Exact binomial tests were used as exploratory checks against a reference proportion of 0.50. Due to the limited and non-probability sample, the results should be interpreted cautiously.

The basic statistical checks are consistent with the descriptive findings. Indicators such as familiarity with the GDPR breach definition, the implementation of technical measures, and awareness of the 72-hour notification deadline show clearly high values. In contrast, indicators such as simulations, the practical application of Guidelines 9/2022, and actual notification of data subjects show clearly low values. This supports the conclusion that organizations are more likely to have baseline legal and technical preparedness than tested practical response mechanisms.

Responses related to actual incident experience and notification obligations further confirm this trend. Only 24.5% of respondents indicate that incidents involving potential personal data breaches have occurred in their

organizations over the past two years, while 22.4% report that they are unable to assess whether such cases have taken place. At the same time, 71.4% are aware of the 72-hour notification deadline, 65.3% report the existence of a written procedure or policy for notifying the Commission for Personal Data Protection (CPDP), and 79.6% recognize that, under certain conditions, affected data subjects must also be notified. However, only 8.2% indicate that notification of data subjects has actually been carried out in practice within their organizations. The contrast between the relatively broad awareness of legal requirements and the more limited practical experience suggests that organizations appear better prepared to describe the applicable rules than to execute the full sequence of actions in real situations characterized by tight deadlines, incomplete information, and the need for rapid internal coordination. In the same direction, 67.3% consider a standardized template for notifying data subjects of a breach to be necessary. Key indicators related to notification are summarized in Table 4.

TABLE IV. NOTIFICATION PRACTICES IN THE EVENT OF A SECURITY BREACH

Indicator	n	%
Organizations with incidents in the past two years	12	24.5
Awareness of the 72-hour notification deadline	35	71.4
Written procedure/policy for notification to the Commission for Personal Data Protection	32	65.3
Awareness of the obligation to notify data subjects	39	79.6
Actual notification of data subjects in practice	4	8.2
Need for a standardized notification template	33	67.3

Particularly indicative are the results concerning awareness and application of Guidelines 9/2022 of the European Data Protection Board and the methodology of the Commission for Personal Data Protection for determining the level of risk in personal data breaches. Partial or full awareness of Guidelines 9/2022 was reported by 69.4% of respondents; however, only 14.3% have actually used them in incident notification. Nevertheless, among those who are at least partially familiar with the Guidelines, 76.5% consider them useful, and the same proportion indicate the need for additional practical guidance from the national supervisory authority. Even more indicative are the findings related to the methodology of the Commission for Personal Data Protection. Only 46.9% are aware of its existence and content; among them, 47.8% perceive it as useful, 56.5% believe that it should be revised and simplified, 73.9% indicate the need for additional explanations and training, 91.3% would participate in specialized training, and 95.7% regard the publication of such a methodology as a useful initiative. These results suggest that the issue does not lie in the rejection of methodological and regulatory instruments, but rather in their limited practical applicability and the need to translate them into more accessible procedures, examples, and actionable models. The data on the guidelines, the methodology, and the expressed need for additional support are summarized in Table 5.

TABLE V. GUIDELINES 9/2022, METHODOLOGY OF THE COMMISSION FOR PERSONAL DATA PROTECTION AND NEED FOR ADDITIONAL SUPPORT

Indicator	n	%
Awareness (at least partial) of Guidelines 9/2022	34/49	69.4
Application of Guidelines 9/2022 in incident notification	7/49	14.3
Perception of Guidelines 9/2022 as useful (among those aware)	26/34	76.5
Awareness of the methodology of the Commission for Personal Data Protection	23/49	46.9
Perception of the methodology as useful (among those aware)	11/23	47.8
Opinion that the methodology should be simplified	13/23	56.5
Indicated need for additional training	17/23	73.9
Willingness to participate in specialized training	21/23	91.3
Perception of the publication of the methodology as a useful initiative	22/23	95.7

Additional questions related to training, resources, and self-assessment of preparedness further confirm the existence of a clear distinction between basic and advanced organizational readiness. Regular training on GDPR and incident response is conducted in 53.1% of organizations, onboarding training on personal data protection for new employees is provided in 59.2%, cybersecurity training for information technology (IT) teams is implemented in 57.1%, and two-factor authentication is used in 63.3% of cases. At the same time, simulations and training exercises are conducted comprehensively in only 26.5% of organizations. Self-assessment of preparedness also reveals differences across employee groups. The highest level of preparedness is attributed to IT teams, with 73.5% rating their level as “good” or “very good,” followed by legal departments and consultants at 59.2%, while among other employees handling personal data this share is significantly lower, at 42.9%. Furthermore, 65.3% of respondents do not consider the public and private sectors to be equally well prepared, 75.5% indicate that their organizations follow news and guidance on the topic, and 79.6% express the need for more practical examples from competent authorities. These findings suggest that the most vulnerable aspect of incident response is not solely the technical infrastructure, but the organization’s ability to consistently apply knowledge across all units.

In summary, the obtained results suggest that Bulgarian organizations demonstrate a relatively high level of formal awareness regarding personal data breaches; however, this awareness is not equally supported by a well-developed level of practical preparedness. A clear discrepancy exists between the presence of basic legal knowledge and documented internal rules, on the one hand, and the ability to ensure a rapid, coordinated, and procedurally sound response to actual incidents, on the other. This finding is consistent with the scientific and applied literature discussed in the theoretical section, which emphasizes that effective incident response extends beyond formal

compliance and requires preparation, internal coordination, monitoring, training, testing, and subsequent organizational analysis. The empirical results indicate that the main challenges lie precisely at the level of operational execution and practical implementation, highlighting the need for clearer procedures, practical guidance, and more targeted training initiatives.

IV. CONCLUSIONS

The present study demonstrates that Bulgarian organizations exhibit a relatively good level of initial awareness regarding personal data breaches and the key obligations arising from the applicable legal framework. A significant proportion of organizations have appointed a Data Protection Officer, have defined internal responsibilities, implement technical security measures, and are aware of their obligations to notify the supervisory authority. At the same time, however, the results clearly indicate that practical preparedness for incident management remains unevenly developed. The less developed elements are precisely those that transform formal compliance into an effective response capability—namely, incident tracking systems, access monitoring, regular testing, simulations, practically applicable methodologies, and adequately trained personnel beyond specialized legal and IT functions.

The obtained data provide grounds to conclude that the main issue is not the absence of a regulatory framework or a complete lack of awareness, but rather the difficulty in translating requirements into clear internal actions and consistent organizational practices. Particularly indicative in this regard are the limited practical application of Guidelines 9/2022, the low level of awareness of the methodology of the Commission for Personal Data Protection, and the clearly expressed need for additional explanations, templates, practical guidance, and training.

Therefore, it can be argued that organizations require not only legal information, but also an applicable response model that integrates early incident detection, risk assessment, internal role allocation, documentation, notification, and post-incident analysis into a coherent and consistent process.

Several limitations should be noted. First, the sample includes 49 valid responses and has a non-probability character; therefore, the results should not be interpreted as nationally representative of all organizations in Bulgaria. Second, due to the dissemination procedure, the exact number of persons reached by the invitation cannot be determined, and a response rate was not calculated. Third, the data are based on respondents' self-assessment, which means that differences may exist between declared practices and actual organizational behavior during a specific incident. Despite these limitations, the results provide a useful empirical basis for identifying recurring difficulties and for formulating subsequent recommendations for managing responses to personal data breaches.

Nevertheless, the conducted research provides a valuable empirical basis for the formulation of future

recommendations, the development of practically oriented models for responding to personal data breaches, and further comparative studies on the characteristics of national notification procedures across different European Union Member States. In this sense, the study fulfills its primary scientific objective—to identify key challenges in organizational practice and to indicate directions for the development of more effective solutions for managing incidents involving personal data.

ACKNOWLEDGMENTS

The present paper was prepared as a result of the scientific research activities conducted within the scientific project “Managing Personal Data Breach Response Processes in the Activities of Organisations in the Republic of Bulgaria,” financed by the Bulgarian National Science Fund under the “Competition for financing fundamental scientific research – 2024,” Contract No. KII-06-H85/10 (BG-175467353-2024-11-0016-C01), dated 05.12.2024.

REFERENCES

- [1] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 (General Data Protection Regulation),” *Official Journal of the European Union*, Apr. 27, 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- [2] European Data Protection Board, “Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0,” Mar. 28, 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v_2.0_en.pdf
- [3] European Data Protection Board, “Guidelines 01/2021 on examples regarding personal data breach notification, Version 2.0,” Dec. 14, 2021. [Online]. Available: https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adapted_en.pdf
- [4] Commission Nationale de l’Informatique et des Libertés, “Notify a personal data breach,” May 24, 2018. [Online]. Available: <https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles>
- [5] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, “Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile,” *NIST Special Publication 800-61r3*, Apr. 2025. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>
- [6] European Union Agency for Cybersecurity, “ENISA threat landscape 2020 – data breach,” Oct. 20, 2020. [Online]. Available: <https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Data%20Breach%20A4.pdf>
- [7] I. A. Tøndel, M. B. Line, and M. G. Jaatun, “Information security incident management: Current practice as reported in the literature,” *Computers & Security*, vol. 45, pp. 42–57, 2014, doi: [10.1016/j.cose.2014.05.003](https://doi.org/10.1016/j.cose.2014.05.003).
- [8] Supreme Court of Cassation of the Republic of Bulgaria, “Actions in case of a personal data security breach,” internal procedure, 2023. [Online]. Available: <https://www.vks.bg/dokumenty-zzld/vks-zapoved-2023-808-procedura-narushenie.pdf>
- [9] European Data Protection Board, “How to notify a data breach to your Data Protection Authority (DPA),” n.d. [Online]. Available: https://www.edpb.europa.eu/notify-data-breach_en
- [10] Data Protection Commission, “Breach Notification,” n.d. [Online]. Available: <https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification>
- [11] Commission Nationale de l’Informatique et des Libertés, “Cybersecurity 2024,” 2024. [Online]. Available: https://www.cnil.fr/sites/cnil/files/2024-05/cnil_cybersecurity_2024_en.pdf
- [12] Agencia Española de Protección de Datos, “Notification of a personal data breach to the Supervisory Authority,” Dec. 11, 2025. [Online]. Available: <https://www.aepd.es/en/rights-and-duties/fulfill-your-duties/measures-compliance/notification-of-personal-data-breach-to-the-supervisory-authority>

III

SUSTAINABLE ENERGY ENGINEERING AND APPLICATIONS

Energy Cost Pressure, Agricultural Input Prices and Farm Economic Resilience in Selected Market Farm Types: Comparative Evidence from Bulgaria and the EU-27

Ivan Byanov

dept. Economic theory and International economic relations
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
iv.byanov@ts.uni-vt.bg

Nevena Byanova

dept. Economic theory and International economic relations
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
n.byanova@ts.uni-vt.bg

Abstract - The paper examines the relationship between energy cost pressure, agricultural input prices and farm economic resilience in Bulgaria compared with the EU-27 average. The empirical design combines three groups of official data sources: Eurostat non-household electricity prices, Eurostat agricultural input price indices, and Farm Sustainability Data Network (FSDN) standard results for selected specialised market farm types. The focus is on Bulgaria and the EU-27 average, with farm-type outcomes compared, energy-price dynamics analysed, and agricultural input-price developments traced for 2020–2024. Methodologically, the study applies a comparative descriptive and relational approach. Farm-type indicators are derived through weighted aggregation across economic size classes. Four indicators are used to assess resilience: income margin, energy cost share, intermediate consumption intensity and liabilities-to-assets ratio.

The results show that the Bulgarian case cannot be interpreted as a uniform deviation from the EU-27 average. Instead, the evidence points to a strongly differentiated resilience profile across farm types. Milk and other grazing livestock display comparatively strong resilience, granivores improve between 2021 and 2023, while fieldcrops and especially mixed farms weaken markedly by 2023. The findings suggest that the main transmission mechanism operated less through direct energy cost share and more through broader pressures on intermediate consumption and financial sustainability. The paper concludes that agriculture should not be treated as a homogeneous sector when assessing resilience to energy and input price shocks, and that policy responses should be more sensitive to farm-type heterogeneity.

Keywords - agriculture, agricultural input costs, Bulgaria, energy prices, farm resilience

I. INTRODUCTION

The economic environment in which European agriculture operates has become increasingly shaped by the interaction of climate policy, energy market volatility and geopolitical instability. Farmers operate under simultaneous pressure from rising costs, climate change and supply-chain disruptions. In the European Union, the green transition is framed by the European Green Deal, which defines climate neutrality by 2050 as a strategic objective [1], and by the European Climate Law, which translates this objective into binding commitments and intermediate emissions-reduction targets [2]. Within this broader framework, the Farm to Fork Strategy places agriculture and the food system at the centre of the transition towards sustainability, emphasising the need to reconcile environmental objectives, food security and economic viability [3]. Further European Green Deal is strongly aligned with SDG 7, SDG 12 and SDG 13, which makes the analysis of agricultural cost pressure and resilience especially relevant from both an economic and a sustainability perspective [4].

Simultaneously, the agricultural sector has been exposed to a much more unstable global economic and geopolitical environment. The war in Ukraine triggered what the IEA describes as the first truly global energy crisis, with effects that were especially severe in Europe [5]. For agriculture, this matters not only because of direct fuel and electricity use, but also because the transmission from energy markets to farm costs is amplified through fertilizer production. Ammonia is the starting point for all mineral nitrogen fertilizers, and around 70% of ammonia is used to make fertilizers [6]. FAO monitoring shows that fertilizer prices have observed extreme peaks in 2022 [7]. At the same time, the World Bank continues to identify worsening geopolitical tensions as an upside risk to oil, gas and agricultural price spikes [8].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.107>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Against this background, literature increasingly conceptualises agriculture as a dual energy sector, simultaneously dependent on direct and indirect energy inputs and increasingly involved in renewable energy generation [9]. This perspective treats energy costs not simply as a technical production expense, but as a structural determinant of farm profitability, competitiveness and financial stability [10]. Existing studies also confirm that the burden of energy use in agriculture extends beyond fuel and electricity to fertilizers, chemicals and other intermediate inputs, which broadens the channels through which energy-price shocks affect farm performance [11]. At the same time, research on on-farm renewables suggests that self-generation can reduce operating costs and improve farm autonomy [9].

Within this context, the question of farm economic resilience becomes especially important. Resilience is often linked the capacity to absorb shocks while preserving economic viability and long-term development potential. In this paper, farm resilience is understood as the ability of different farm types to absorb energy- and cost-related shocks while retaining income, containing intermediate cost pressure and preserving financial stability. In the farm-level literature, economic viability is typically associated with the ability to cover operating costs and liabilities, remunerate production factors and sustain investment capacity over time. Evidence from EU dairy farms shows that resilience is structurally differentiated even within one production system: larger scale may improve short-term viability, while long-term viability may remain constrained by indebtedness and other structural pressures [12]. More recent resilience research broadens this view by distinguishing robustness, adaptability and transformability as complementary capacities rather than as a single continuum [13]. Related evidence also suggests that highly specialised farming systems may be less robust under declining input availability, reinforcing the need for farm-type-specific rather than purely aggregate sectoral analysis.

In the Bulgarian context, sustainability-oriented agricultural development is also discussed in relation to structural and institutional constraints, which may affect the capacity of farms to absorb rising production costs [14]. This makes the comparison between Bulgaria and the EU-27 average particularly relevant. While the macro-level shocks affecting agriculture are broadly shared across the Union, their transmission to farms may differ depending on sectoral structure, cost composition, specialisation patterns and financial vulnerability. Therefore, a comparative farm-type perspective is particularly suitable for assessing whether Bulgarian farms faced a different resilience profile than the EU-27 average.

For the price dimension, Eurostat's agricultural price indices provide a suitable framework for tracing changes in the purchase prices of the means of agricultural production [15], while Eurostat's non-household electricity statistics capture the wider energy-price environment relevant for farm businesses [16]. For the farm-level dimension, the Farm Sustainability Data Network provides a particularly

appropriate empirical basis, as it gathers annual farm-level data from a harmonised EU survey and makes it possible to compare results across years, countries, farming types and economic size classes [17]. This dataset supports a differentiated assessment of how cost pressure is transmitted into farm economic performance and financial vulnerability.

The objective of this paper is to examine whether rising energy cost pressure was associated with stronger agricultural input cost pressure and differentiated farm economic resilience in Bulgaria compared with the EU-27 average. The paper addresses three questions: how energy cost pressure evolved in Bulgaria and the EU-27; to what extent this pressure was reflected in agricultural input prices; and how selected specialised market farm types performed under that pressure in terms of income retention, direct energy exposure and cost intensity. In this way, the paper contributes to the literature by linking the broader green-transition and geopolitical context to farm-level evidence on economic resilience in selected market farm types.

II. DATA AND METHODOLOGY

The paper is structured around three empirical blocks. The first examines the macro-level energy cost environment through Eurostat non-household electricity prices. The second traces how this pressure is transmitted into agriculture using Eurostat agricultural input indices with particular attention to the "energy and lubricants" component [18]. The third evaluates farm-type resilience through weighted indicators derived from Farm Sustainability Data Network (FSDN) standard results for selected specialised market farm types, capturing profitability, direct energy exposure, cost intensity and financial vulnerability.

Non-household electricity prices are used as a macro-level proxy for the energy cost environment faced by productive sectors. No harmonised farm-specific energy price series is available at EU level for comparative annual analysis. This indicator does not capture the full energy cost structure of agriculture, but it provides a comparable measure of economy-wide energy price pressure across countries.

The empirical focus is on Bulgaria and the EU-27 average. The core comparative window is 2021–2023, while the energy-price analysis uses the broader 2019–2024 context and the agricultural input-price analysis uses the 2020–2024 period. The FSDN-based farm-type analysis covers five specialised market farm types: fieldcrops, milk, other grazing livestock, granivores and mixed farms. Because the FSDN public database reports standard results by economic size class, farm-type indicators for each country and year were derived through weighted aggregation. The weighting variable was the number of farms represented (SYS02). For each country c , farm type f , year t and size class s , the weighted value of a basic variable X was calculated as $X_{w} = \text{sum}(X_s \times \text{SYS02}_s) / \text{sum}(\text{SYS02}_s)$. Size classes with missing public values were excluded from the relevant

denominator. The reported resilience indicators were then derived from weighted values rather than from direct averages of row-level ratios, which avoids distortions from averaging already-transformed size-class ratios.

The four reported resilience indicators are defined as follows: income margin = $SE420_w / SE131_w$; energy cost share = $SE345_w / SE275_w$; intermediate consumption intensity = $SE275_w / SE131_w$; and liabilities-to-assets ratio = $SE485_w / SE436_w$. Higher income margins indicate stronger income resilience, whereas higher values of the other three indicators generally reflect stronger direct energy exposure, greater cost absorption relative to output, and greater financial vulnerability, respectively.

The four indicators were selected to capture complementary dimensions of economic resilience at farm-type level. Income margin reflects the capacity to retain income from output under cost pressure. Energy cost share measures direct exposure to energy-related costs within intermediate consumption. Intermediate consumption intensity captures the broader degree to which output is absorbed by current production costs. Finally, the liabilities-to-assets ratio reflects financial vulnerability and leverage. Taken together, these indicators provide a compact but multidimensional view of farm-type economic resilience under adverse cost conditions.

The empirical design is comparative and exploratory rather than causal. The paper does not claim to identify strict causal effects between macro-level energy prices and farm-level outcomes. Instead, it examines whether the observed movements in electricity prices, agricultural input prices and farm-type economic indicators display comparative patterns across Bulgaria and the EU-27.

The analysis also faces important data constraints. First, non-household electricity prices do not capture the entire energy-related burden of agriculture, which also includes fuel, transport, fertilisers and other cost channels. Second, the public FSDN database contains missing or suppressed values for some Bulgarian farm-type size classes, which limits the completeness of coverage in selected categories. These limitations do not invalidate the comparative exercise, but they require cautious interpretation of farm-type results.

III. ENERGY COST PRESSURE IN BULGARIA AND THE EU-27

Non-household electricity prices increased sharply in both Bulgaria and the EU-27 during the energy shock period. In PPS terms, Bulgaria remained above the EU-27 average throughout 2019–2024 and experienced a markedly stronger increase at the peak of the shock. In the EU-27, the PPS-based price rose from 0.1665 in 2019 to 0.2834 in 2022 and 0.2931 in 2023, before declining to 0.2598 in 2024. In Bulgaria, it increased from 0.2196 in 2019 to 0.4249 in 2022, then fell to 0.3165 in 2023 and 0.2725 in 2024. Although prices declined after the peak, the correction remained incomplete, as both Bulgaria and the EU-27 stayed above pre-shock levels by 2024 (Fig. 1). Overall, Bulgarian producers operated in a comparatively

less favourable macro-level energy price environment, especially during the peak shock years.

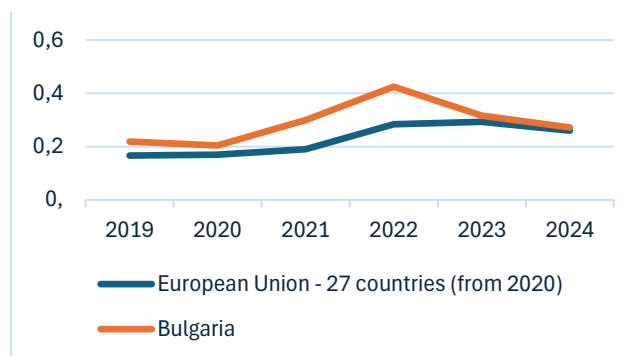


Fig. 1. Non-household electricity prices in Bulgaria and the EU-27, PPS, 2019–2024

The evidence establishes the broader energy cost environment within which agricultural producers operated during the shock period. However, higher electricity prices at the level of non-household consumers do not automatically imply an identical response within agriculture. The next analytical step is therefore to examine whether this macro-level energy pressure was transmitted into the agricultural production environment through higher input prices. In this context, particular attention is paid to the component “energy and lubricants”, as it captures the most direct energy-related channel within agricultural input costs. Comparing this component with total input prices also makes it possible to assess whether the energy shock had a distinct and disproportionate effect on agricultural cost structures in Bulgaria and the EU-27.

IV. TRANSMISSION INTO AGRICULTURAL INPUT PRICES

The agricultural input price evidence does not indicate a direct one-to-one transmission of the stronger Bulgarian macro-level energy shock into a proportionally stronger agricultural energy-input shock. According to Eurostat agricultural input price indices, both Bulgaria and the EU-27 experienced a clear peak in 2022, yet the increase in the “energy and lubricants” component was considerably stronger in the EU-27 average than in Bulgaria.

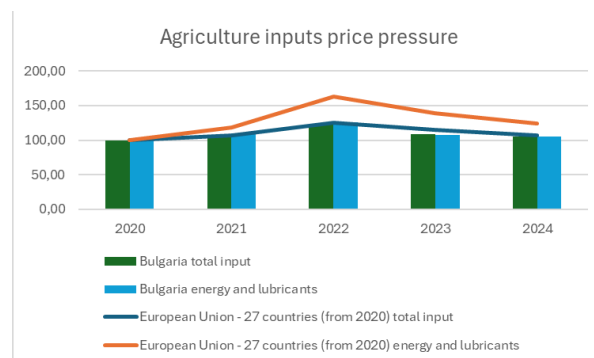


Fig. 2. Agricultural input prices in Bulgaria and the EU-27: total inputs and energy and lubricants, 2020=100, 2020–2024

Fig. 2 illustrates a sharp rise in agricultural input price pressure in both Bulgaria and the EU-27, culminating in a clear peak in 2022. In each case, the index for energy and lubricants increased more strongly than the aggregate input index, indicating that energy-related costs constituted a major channel through which the broader price shock affected agriculture. This divergence, however, is more pronounced at the EU-27 level. In the EU-27, the real index for energy and lubricants increased from 100.00 in 2020 to 162.85 in 2022, whereas the total input index rose to 124.78. In Bulgaria, the corresponding change was less intense: the energy and lubricants index reached 126.04, while the total input index rose to 123.37 in 2022. This pattern suggests that Bulgaria followed the same general upward trajectory, but without experiencing an agricultural energy-price spike of the same magnitude as the EU-27 average. By 2024, both series had moved back closer to the 2020 baseline, although the adjustment was still incomplete, particularly in the EU-27 energy and lubricants component. Taken together, these results provide the empirical basis for examining whether the observed input-price pressure was associated with weaker farm economic resilience across the selected market farm types.

This suggests that macro-level energy price pressure and sector-level agricultural input price transmission were related, but not mechanically identical. Bulgaria followed the general upward pattern, yet the agricultural energy-related input-price spike was less pronounced than the EU-27 average. The result is analytically important because it indicates that stronger macro-level energy pressure in Bulgaria did not automatically imply stronger sector-level agricultural input-price escalation.

V. FARM-TYPE RESILIENCE UNDER COST PRESSURE

Table 2 reports weighted farm-type resilience indicators derived from FSDN standard results. The interpretation of these indicators follows the broader literature linking farm income retention, direct energy exposure, cost absorption and financial position to economic resilience.

Fieldcrop farms show the clearest deterioration in Bulgaria. In 2021, the Bulgarian income margin was slightly above the EU-27 benchmark (0.380 versus 0.368), but by 2023 it had fallen sharply to 0.031, compared with 0.226 in the EU-27. At the same time, Bulgarian intermediate consumption intensity rose from 0.380 to 0.639, converging to the EU-27 level, while the liabilities-to-assets ratio increased from 0.216 to 0.251. This

combination indicates a sharp deterioration in cost intensity and a substantial weakening of the capacity to retain income under pressure.

Milk farms display one of the strongest Bulgarian resilience profiles. The income margin increased from 0.429 in 2021 to 0.483 in 2023, whereas the EU-27 average declined from 0.253 to 0.215. Bulgarian milk farms also maintained lower intermediate consumption intensity and lower liabilities-to-assets ratios than the EU-27 average in both years. Although the share of direct energy costs remains higher in Bulgaria, stronger income retention, relatively lower cost intensity and a manageable level of indebtedness outline a comparatively resilient profile for milk farms.

Other grazing livestock farms show the strongest income performance in the Bulgarian sample. Income margin rose from 0.802 to 0.906, compared with a decline from 0.363 to 0.310 in the EU-27. Intermediate consumption intensity remained below the EU-27 level in both years, and the liabilities-to-assets ratio improved strongly from 0.212 to 0.104. These results indicate very strong apparent resilience, based on high income margins and relatively limited cost absorption, but the interpretation should remain cautious due to the incomplete coverage of Bulgarian size classes in the public database for this category.

Granivores improved in both Bulgaria and the EU-27, but the Bulgarian improvement is more pronounced. The Bulgarian income margin rose from 0.125 to 0.234, slightly overtaking the EU-27 value in 2023. At the same time, energy cost share declined from 0.080 to 0.071, intermediate consumption intensity declined from 0.749 to 0.652, and the liabilities-to-assets ratio improved from 0.272 to 0.237. Taken together, these changes suggest a strengthening resilience profile within the represented Bulgarian sample, associated with improved income retention, lower cost intensity and reduced direct energy burden.

Mixed farms show one of the strongest cases of deterioration. In Bulgaria, the income margin fell from 0.353 to 0.041, whereas the EU-27 declined only from 0.222 to 0.171. Intermediate consumption intensity increased sharply from 0.537 to 0.791, and the liabilities-to-assets ratio rose from 0.278 to 0.561. This combination indicates a simultaneous weakening of income retention, stronger cost absorption and a marked deterioration in the balance-sheet position of Bulgarian mixed farms by 2023.

Table 2. Weighted farm-type resilience indicators in Bulgaria and the EU-27, 2021 and 2023

Farm type	Country	IM 2021	IM 2023	ECS 2021	ECS 2023	ICI 2021	ICI 2023	LAR 2021	LAR 2023
Fieldcrops	Bulgaria	0.380	0.031	0.182	0.161	0.380	0.639	0.216	0.251
	EU-27	0.368	0.226	0.142	0.138	0.538	0.639	0.148	0.144
Milk	Bulgaria	0.429	0.483	0.112	0.104	0.569	0.578	0.085	0.173
	EU-27	0.253	0.215	0.088	0.089	0.646	0.674	0.224	0.211

Other grazing livestock	Bulgaria	0.802	0.906	0.102	0.107	0.682	0.708	0.212	0.104
	EU-27	0.363	0.310	0.096	0.099	0.718	0.743	0.112	0.110
Granivores	Bulgaria	0.125	0.234	0.080	0.071	0.749	0.652	0.272	0.237
	EU-27	0.158	0.226	0.058	0.058	0.744	0.671	0.317	0.287
Mixed	Bulgaria	0.353	0.041	0.142	0.145	0.537	0.791	0.278	0.561
	EU-27	0.222	0.171	0.102	0.105	0.677	0.708	0.192	0.186

Abbreviations: IM = income margin; ECS = energy cost share; ICI = intermediate consumption intensity; LAR = liabilities-to-assets ratio.

Overall, Table 2 points to distinct resilience profiles across farm types in Bulgaria relative to the EU-27. The most pronounced weakening is observed in fieldcrops and mixed farms, whereas milk, other grazing livestock and, to some extent, granivores show more resilient dynamics.

VI. DISCUSSION

Beyond its agricultural-economic contribution, the paper is also relevant to data-driven system analysis because it demonstrates how harmonised public datasets can be combined into a structured framework for monitoring resilience under external shocks. In this sense, the study contributes to indicator-based analytical support for policy design, sectoral monitoring and evidence-based decision environments.

The comparison between Bulgaria and the EU-27 suggests that farm resilience under energy- and cost-related pressure cannot be inferred directly from the macro-level energy price environment alone. Although Bulgaria faced a less favorable energy price context in PPS terms, this did not translate into a uniformly weaker agricultural outcome. Instead, the evidence points to a differentiated transmission process, in which the effects of energy and input price shocks varied according to the production specialization, cost structure and financial position of farm types. This is important because aggregate agricultural indicators may conceal substantial internal differences in the capacity of farms to absorb external shocks.

The observed differences are consistent with a pattern in which cost pressure is reflected through broader changes in intermediate consumption and financial pressure. The impact of the energy-price shock was reflected in broader changes in intermediate consumption and financial pressure. In this sense, energy cost pressure should be interpreted as part of a wider inflationary environment affecting agriculture through multiple input channels. Farm types with stronger income retention and more stable cost absorption were better positioned to withstand this pressure, whereas those with rising intermediate consumption intensity or increasing leverage displayed weaker resilience. Therefore, the relationship between macro-level energy prices and farm-level outcomes is shaped by structural characteristics such as input dependence, cost absorption capacity and balance-sheet vulnerability.

From a policy perspective, these findings suggest that resilience-enhancing measures should not be designed only

at the aggregate agricultural level. A more targeted approach is needed, considering the specific vulnerabilities of different farm types. For farms with rising intermediate consumption intensity, support may focus on cost efficiency, input substitution and technological modernization. For farms with increasing financial vulnerability, measures related to liquidity, investment capacity and debt management may be more relevant. Thus, strengthening resilience requires not only reducing direct energy exposure, but also improving cost management, financial sustainability and adaptive capacity across production systems.

VII. CONCLUSION

The paper demonstrates that energy cost pressure, agricultural input price dynamics and farm-type resilience can be meaningfully linked within a comparative Bulgaria - EU-27 framework using official Eurostat and FSDN data. The Bulgarian case does not point to a uniformly weaker or stronger position relative to the EU-27 average; instead, it reveals substantial variation across farm types.

Fieldcrops and mixed farms appear the most vulnerable, while milk and other grazing livestock show comparatively strong resilience and granivores improve over the period. This suggests that the effects of energy- and cost-related pressure were transmitted through broader changes in intermediate consumption and financial sustainability. The findings therefore indicate that policies aimed at strengthening resilience should be more differentiated and should account for variation in production specialization, cost structure and financial vulnerability across farm types.

Future research could extend the analysis to a wider country sample, additional farm types and more detailed evidence on farm-level adaptation strategies. Further work is also needed on the mechanisms through which energy-price shocks are transmitted into cost pressure and financial stress in agriculture, to identify more precisely which farm types are most exposed and what forms of support are likely to be most effective.

REFERENCES

- [1] European Commission, "The European Green Deal," COM(2019) 640 final, 2019. [Online]. Available: EUR-Lex PDF
- [2] European Union, "Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality (European Climate

- Law),” 2021. [Online]. Available: [Regulation - 2021/1119 - EN - EUR-Lex](#)
- [3] European Commission, “A Farm to Fork Strategy for a fair, healthy and environmentally friendly food system,” COM(2020) 381 final, 2020. [Online]. Available: [f2f_action-plan_2020_strategy-info_en.pdf](#)
- [4] P. Koundouri, A. Alamanos, A. Plataniotis, C. Stavridis, K. Perifanos, and S. Devves, “Assessing the sustainability of the European Green Deal and its interlinkages with the SDGs,” *npj Climate Action*, vol. 3, 2024, DOI: [10.1038/s44168-024-00104-6](#).
- [5] International Energy Agency, “Russia’s War on Ukraine,” [Online]. Available: [Russia's War on Ukraine – Topics - IEA](#)
- [6] International Energy Agency, “Ammonia Technology Roadmap.” Paris, France: IEA, 2021. [Online]. Available: [Ammonia Technology Roadmap](#)
- [7] FAO, “Fertilizer market developments,” 2025. [Online]. Available: [Fertilizer market developments](#)
- [8] World Bank, “Commodity Markets Outlook,” Apr. 2025. Washington, DC, USA: World Bank, 2025. DOI: 10.1596/43036.
- [9] R. Ryś-Jurek, “On-Farm Production of Renewable Energy in 2014–2022,” *Energies*, vol. 17, no. 21, art. 5395, 2024, DOI: 10.3390/en17215395.
- [10] A. Strzelecka, E. Szafraniec-Siluta, and D. Zawadzka, “Energy Costs and the Financial Situation of Farms in the European Union,” *Energies*, vol. 18, no. 23, art. 6299, 2025, DOI: 10.3390/en18236299.
- [11] L. Wicki, H. Dudek, A. Parzonko, D. Kusz, and K. Naglis-Liepa, “Factors Influencing the Productivity of Direct Energy Inputs in EU Agriculture,” *Sustainability*, vol. 17, no. 3, art. 1217, 2025, DOI: 10.3390/su17031217.
- [12] A. Wilczyński and E. Kołoszycz, “Economic Resilience of EU Dairy Farms: An Evaluation of Economic Viability,” *Agriculture*, vol. 11, no. 6, art. 510, 2021, DOI: 10.3390/agriculture11060510
- [13] J. Martín-García, J. A. Gómez-Limón, and A. Menor-Campos, “Farms’ economic resilience: assessment, drivers and policy-making,” *Environmental and Sustainability Indicators*, vol. 27, art. 100740, 2025, DOI: 10.1016/j.indic.2025.100740
- [14] Y. Toneva, “Production and Consumption of Organic Food in the Republic of Bulgaria - Problems and Prospects,” in *Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference*, vol. 1, pp. 537–545, 2025, DOI: 10.17770/etr2025vol1.8674.
- [15] Eurostat, “Price indices of the means of agricultural production, input (2020 = 100) - annual data,” online data code: APRI_PI20_INA. DOI: 10.2908/apri_pi20_ina.
- [16] Eurostat, “Electricity prices for non-household consumers - bi-annual data (from 2007 onwards),” online data code: NRG_PC_205. DOI: 10.2908/nrg_pc_205.
- [17] European Commission, “FSDN public database / Farm economy focus,” Agri-food Data Portal, Brussels, 2025. Available: [European Commission | Agri-food data portal | FSDN Database](#)
- [18] Eurostat, “Price indices of the means of agricultural production, input (2020 = 100) — annual data,” dataset apri_pi20_ina, European Commission, Luxembourg, 2025. DOI: 10.2908/APRI_PI20_INA

Bulgaria's Hybrid Energy Model: Legal Aspects of Systemic Sustainability

Olga Borisova

Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
olga.borisova@vfu.bg

Abstract—This study analyzes the critical interaction between centralized nuclear power capacities and emerging decentralized energy communities within the context of the full liberalization of the Bulgarian energy market by 2026. The primary focus is directed toward the regulatory dichotomy between the Energy Act, which ensures systemic security through base-load capacities, and the Energy from Renewable Sources Act, which introduces decentralized entities and derogates the traditional "vertical" energy model. The analysis establishes that the transition to a free market fundamentally alters the status of the Kozloduy Nuclear Power Plant—moving it from a strategic asset with administrative quotas to an active market participant exposed to price volatility and in need of new financial instruments, such as Contracts for Difference. In parallel, the Energy from Renewable Sources Act legitimizes the figures of the "active consumer," the "citizen energy community," and the "independent aggregator," providing them with streamlined administrative regimes and energy-sharing rights. The research identifies a significant regulatory vacuum regarding pecuniary liability for imbalances and the allocation of systemic sustainability costs. It highlights the legal antinomy between the priority grid access granted to renewable energy sources communities and the technological inertia of nuclear capacities, which often leads to the improper socialization of individual costs within the overall system price. In conclusion, specific legislative measures are proposed to achieve regulatory synergy, including the introduction of "flexible grid contracts," the transformation of network services toward capacity-based fees (per kW), and the integration of decentralized sources under the direct operational control of the system operator. The author substantiates the thesis that the sector's sustainability depends on transitioning from a model of parallel existence toward the legally regulated functional integration of generating capacities.

Keywords— communities, dichotomy, nuclear, sustainability.

I. INTRODUCTION

The legal framework of the Bulgarian energy sector faces a unique challenge: reconciling the strictly regulated

regime of strategic nuclear capacities with the liberal legal status of renewable energy communities. While the operational units and the project for new reactors at the Kozloduy NPP require targeted regulatory frameworks and state guarantees for risk management, the transposition of Directive (EU) 2018/2001 via the Energy from Renewable Sources Act (ERSA) introduces decentralized entities that derogate from the traditional "vertical" energy model.

By 2026, legal discourse has evolved from passive regulatory monitoring toward the conceptual construction of a hybrid model. This model aims to ensure regulatory interoperability between strategic centralized capacities (such as NPPs, TPPs, etc.), which guarantee systemic stability, and the subjective right of end-users to energy autonomy and market participation through decentralized production. [1]

The analysis identifies a significant regulatory dichotomy between the Energy Act (EA), focused on systemic security and base-load assurance, and the Energy from Renewable Sources Act (ERSA), directed toward decentralization and sustainability. While the EA establishes nuclear energy as a fundamental guarantor of security, the ERSA reconfigures the linear "producer-consumer" model into a dynamic market ecosystem.

Critical legal conflicts have been identified regarding the allocation of financial responsibility for balancing, priority access to grid capacity, and the absence of a unified tariff model for grid solidarity. [2]

The report concludes that the current regulatory framework treats centralized and decentralized production as mutually exclusive regimes rather than components of an integrated system. In conclusion, it is emphasized that the sustainability of the energy sector depends on the transition from a model of parallel operation to a legally regulated functional integration of diverse generating capacities.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.24>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

II. LEGAL REGIME OF CENTRALIZED CAPACITIES (ENERGY ACT)

The legal framework for centralized capacities in Bulgaria is based on the concepts of energy security and continuity of supply. The primary focus here lies on a hierarchical management structure, where the State occupies a central role through strategic planning and regulation.

1. Status of Base-load Capacity and "Critical Infrastructure"

Pursuant to the EA, large-scale centralized capacities (primarily Nuclear Power Plants) function not merely as commercial participants, but as guarantors of national security. Article 69 of the EA imposes an obligation upon energy enterprises to act in the public interest, ensuring the protection of critical infrastructure, continuity of supply, and environmental preservation.

A key aspect of the EA is the regulation of the powers of the Electricity System Operator (ESO). In a legal sense, the operator possesses imperative powers to mandate changes in the load of centralized capacities. A conflict arises from the fact that nuclear reactors, by technological design, have limited maneuverability—a fact reflected by the legislator through the provision of dispatching priority as "base-load."

Nuclear energy is defined as a priority via the mechanism of Art. 4, Para. 2, Item 3 of the EA. This provision empowers the Minister of Energy to propose a list of strategic objects of national importance to the Council of Ministers. In exercise of this power, via Council of Ministers Decree No. 181 of 2009 [1], the "Kozloduy" NPP and activities related to radioactive waste management and nuclear fuel have been classified as strategic objects and activities.

The integration of new nuclear capacities into the national energy mix after 2030 is established as a fundamental prerequisite in the draft updated National Integrated Energy and Climate Plan (NECP), developed in accordance with Regulation (EU) 2018/1999.

The implementation process for these projects is subject to a complex licensing regime, integrating the norms of the EA and the Act on the Safe Use of Nuclear Energy (ASUNE). Legally, these capacities are burdened with strict commitments to provide system services that ensure the inertial reserve of the Electric Power System (EPS). In fulfillment of its obligations to guarantee systemic security, the Electricity System Operator (ESO):

- Enters into transactions for additional services (pursuant to Art. 83 and Art. 91 of the EA) to maintain real-time balance;
- Conducts tender procedures for the procurement of frequency restoration reserves and exchange capacities (Art. 105, Para. 1 and 2 of the EA);
- Organizes auctions to guarantee future availability, including from storage facilities, to complement the operation of base-load capacities.

The Capacity Mechanism transforms the legal framework of the market by establishing "availability" as an independent tradable product. In accordance with Article 22 of Regulation (EU) 2019/943, its implementation

requires notification to the European Commission for compatibility with State Aid rules.

The introduced emission limit of 550 g CO₂/kWh normatively restricts fossil fuels while simultaneously affirming nuclear energy as a critical base-load capacity. To avoid overcompensation (double funding), auctions under Art. 105 of the EA must be strictly coordinated with Contracts for Difference (CfDs).

Concurrently, through the independent aggregator, energy communities are integrated into the capacity market. This introduces the legal innovation of "Demand Response," where "unconsumed energy" acquires the legal and economic value of provided capacity.

2. Electricity Transactions under Market Liberalization

The transition to full market liberalization in 2026 fundamentally reshapes the EA, terminating the functions of the "Public Supplier" (NEK EAD) and repealing the administrative quotas for the Kozloduy NPP under Art. 93a of the EA. A restriction on entering into new long-term contracts is introduced, prohibiting state aid for coal-fired power plants; such agreements are permitted only for renewable sources pursuant to Art. 93a, Para. 3 of the EA. Regarding nuclear capacities (NPP), the legal impact of these amendments is manifested in the following areas:

2.1. Derogation of Quota Allocation (Art. 93a of the EA)

With the abolition of the regulated market for end-users, the mechanism under Art. 93a, Para. 1 of the EA—whereby the Energy and Water Regulatory Commission (EWRC/KEVR) determined mandatory purchase quotas from the Kozloduy NPP at preferential prices—loses its legal basis.

- **Restrictions on Long-term Contracts:** According to the new wording of Art. 93a, Para. 2 and Para. 3, the legislator introduces a mandatory prohibition on concluding new long-term contracts for the purchase of energy and availability, unless they concern production from renewable sources. This norm aims to prevent unlawful state aid and promote market competition.

- **Operational Flexibility:** The provision of Art. 93a, Para. 4 limits changes to the Trade Portfolio Schedules (TPS) of high-efficiency energy producers to the scope of Art. 73, aiming to ensure grid stability.

- **Trading Horizon:** The restriction introduced in Art. 93a, Para. 5 for agreements with a term of up to two years on an organized exchange market (for non-RES producers) positions the NPP as an active market participant, but with a fixed time horizon for risk hedging.

2.2. Legal and Economic Consequences after the Cessation of Household Subsidies

The termination of the obligation to "subsidize" household consumers through administrative prices transforms the NPP into a fully market-based entity. Pursuant to Art. 100 of the EA, the entire available quantity of energy must be realized on the Independent Bulgarian Energy Exchange (IBEX).

- **Legal Risk:** Shifting to full exchange-based realization exposes base-load capacities to sharp market fluctuations. In this context, the institutionalization of Contracts for Difference (Art. 36b) becomes a critical legal

instrument for ensuring the financial sustainability of new nuclear projects as a protection mechanism against price volatility. [3]

2.3. Legal Analysis of Changes in the Functions of the "Security of the Electricity System Fund" (SESF)

Within the legal architecture of the Bulgarian energy market, the SESF functions as a specialized body for managing financial flows aimed at compensating deficits arising from regulatory obligations. According to the amendments to Art. 36b, Para. 1 of the EA, the Fund's resources are earmarked and expended for:

- **Covering Public Supplier Costs:** Regulating deficits resulting from the purchase of energy under long-term contracts and preferential prices, including for past periods in accordance with EWRC decisions (Art. 36b, Para. 1, Item 1).
- **Payment of Premium Contracts:** Financing the "premium" mechanism provided to producers with an installed capacity exceeding 500 kW (pursuant to the ERSA), which replaces preferential prices and integrates producers into the market environment (Item 2).
- **Servicing Financial Instruments:** Covering interest payments under framework agreements with credit institutions for energy efficiency projects (Item 3).
- **Extraordinary Compensatory Mechanisms:** Implementing state programs to compensate end-users (household and non-household) during critical price levels for electricity and natural gas. Here, the Fund acts as a payment agent for the executive branch (Item 4).
- **Social Protection and Transition to Liberalization:** Providing compensation through end-suppliers to cover part of the costs for low-voltage household consumers. This provision is key in the context of the abolition of the regulated market (Items 5 and 6). [4]

3. The New Role of Final Suppliers (Art. 98a)

Previously, Final Suppliers (the regional Electricity Distribution Companies) were legally obligated to purchase electricity from the Public Supplier (NEK EAD). Following the 2026 amendments to the EA, they transition into standard market traders.

- **Legal Conflict:** This shift creates a market niche for energy communities. If a community produces its own energy, it directly competes with the former "guaranteed" buyers of nuclear power. Legally, this is protected under Art. 18b, Para. 2 of the ERSA, which prohibits discrimination against consumers participating in energy communities.

III. REGULATORY FRAMEWORK FOR DECENTRALIZED INITIATIVES UNDER THE ERSA

While the EA is primarily focused on the systemic stability of conventional capacities, the ERSA regulates the transition toward a distributed energy architecture. The legal framework is determined by the European doctrine of "energy market liberalization."

1. Energy Communities and Self-Consumption

The amendments to the ERSA in December 2023 incorporated key legal definitions that lay the groundwork for decentralization:

1.1. **Citizen Energy Communities (CEC):** The ERSA does not contain a separate regime for CECs, as they are subjects of the general electricity market, whereas the ERSA specifically regulates Renewable Energy Communities (REC).

- A Citizen Energy Community (CEC) is a legal entity whose regulation is integrated into the general electricity market framework via the Energy Act. Pursuant to the definition in § 1, Item 76 of the Additional Provisions of the EA, a CEC is a specific legal entity through which natural persons, local authorities, and small enterprises carry out joint investments in RES capacities. The law guarantees their preferential legal status, including the right to produce, consume, store, and trade energy while maintaining the full scope of their rights as end-customers.

- The regulation of CECs in Bulgarian legislation was introduced through references to the European framework; however, currently, the primary operational rights of CECs are systematized in Art. 4, Para. 2, Item 21 (as part of state policy) and detailed in Art. 92 et seq., concerning the free market and aggregation.

1.2. **Active Customers (Consumers):** The legislator regulates the status of the "end-customer as an active consumer," granting them the right to generate energy for self-consumption, to store it, and to sell the surplus on the market.

Pursuant to § 1, Item 59 of the AP of the ERSA, this is an entity operating on its own premises for whom energy production is not a primary commercial activity (for non-household consumers).

Provisions under Art. 18a, Paras. 1–4 guarantee the right to participate in support schemes and energy markets without the entity losing its status as an end-customer.

The ERSA regulates the legal figure of the "Prosumer." A key aspect is the normative recognition of the right to energy sharing within a single building or community, which necessitates a revision of standard grid service and access contracts.

1.3. **Energy Aggregators:** The ERSA introduces the legal figure of the Independent Aggregator, acting as a commercial intermediary and technological integrator. Its primary function is to pool loads from multiple decentralized sources (active customers and energy communities) and offer them to the market as a single, controllable resource. Legally, the aggregator resolves the issue of high entry barriers to organized electricity markets while assuming joint and several liability for the balancing of the entities within its portfolio.

The legal basis is found in § 1, Item 1a of the AP of the EA (Art. 18). An aggregator is a natural or legal person carrying out aggregation activities. This provision is pivotal as it regulates the right of end-customers to enter into aggregation contracts without requiring the consent of

their electricity supplier—a fundamental point for guaranteeing competition and freedom of contract.

2. Rights of Active Consumers and Grid Access

The regulatory framework for decentralized capacities is aimed at reducing administrative barriers to market entry through the following mechanisms:

2.1. Simplified Administrative Regimes

The introduction of a notification regime (pursuant to Art. 25a of the ERSA) for small installations with a capacity of up to 20 kW for self-consumption. This mechanism replaces the classical permit-based process with a simplified registration procedure intended to accelerate market integration.

Article 25a of the ERSA holds a central position in this streamlined regime by establishing a presumption of consent in the absence of a timely objection from the grid operator. This regulatory intervention aims to overcome the administrative inertia of Electricity Distribution Companies (EDCs) by transforming the grid connection process from bilateral negotiation into a unilateral right of the active customer, limited only by proven technical impossibility of the system.

- **Scope of Application (Para. 1):** The regime applies to installations with a capacity of up to 20 kW located on existing buildings and facilities (including within urbanized territories). This restriction aims to stimulate so-called "rooftop installations," which do not require a change in land-use designation.
- **Procedural Preclusion (Para. 3):** This is the strongest legal instrument in favor of the active customer. If the grid operator (EDC) does not provide a written objection based on a lack of technical capacity within 15 days of the notification, the connection is deemed tacitly approved.
- **Contractual Freedom (Para. 5):** The article stipulates that relations between the customer and the operator are governed by a template contract for access and transmission, the content of which is legally predefined. This limits the ability of EDCs to impose additional administrative or financial burdens.

2.2. Preferential Access and Connection

The ERSA imposes an objective obligation on Distribution System Operators (DSOs) for the priority connection of RES facilities. In practice, this creates a legal antinomy between the imperative norm to promote decentralization and the technical limitations of grid capacity. This often results in grid connection denials due to a lack of available capacity—an issue the ERSA attempts to resolve through mechanisms for sharing the costs of grid modernization.

IV. REGULATORY CONFLICTS AND CHALLENGES

The coexistence of centralized nuclear energy and decentralized communities in Bulgaria is not merely a technical issue but a significant legal challenge. Conflicts arise from the fact that the EA and the ERSA are based on divergent principles of liability and management. [5]

1. Protection Mechanism for "Vulnerable Consumers" (Art. 38d of the EA)

Market liberalization introduces the key legal category of the "vulnerable customer," defined by Article 38d of the Energy Act (EA) and its associated Ordinance. This regulatory framework shifts the model from general social welfare to targeted, individually segmented assistance within a free-market environment. From a legal perspective, this mechanism functions as a regulatory safeguard against price volatility for high-risk groups.

Key aspects of the legal framework:

- **Definition of "Energy Poverty":** Unlike traditional heating benefits, a complex multi-criteria model is introduced here. It accounts not only for disposable income but also for the technical characteristics (energy efficiency) of the dwelling and the health status of the residents.

- **Financial Mechanism:** The compensation of price differences is carried out through the Security of the Electricity System Fund (SESF), with resources directly linked to revenues from the trading of greenhouse gas emission allowances.

2. Legal Regime of Electricity System Balancing in a Liberalized Market

In the context of market liberalization, balancing is transformed from a technical function into a direct financial obligation for all participants.

Pursuant to § 1, Item 3 of the Additional Provisions of the EA, balancing encompasses the set of actions and processes through which the Electricity System Operator (ESO) guarantees the stability of the system's frequency by activating the necessary reserves.

This legal framework aligns with the European "balancing responsibility" principle established in Regulation (EU) 2019/943. The transition to a free market defines the following legal consequences:

- **Termination of Cost Socialization:** The previous mechanism, where imbalance costs were partially diluted within the end-user prices of the regulated market, is abolished.

- **Direct Financial Liability:** The financial burden for deviations from forecast schedules is transferred to the entities that caused them ("cost-causative" principle).

- **Contractual Autonomy:** Market participants are required to settle their balancing responsibility by entering into contracts with the ESO or by joining a licensed Balancing Group.

The mechanism is detailed in the following texts of the Energy Act:

2.1. Universal Balancing Responsibility (Art. 102 of the EA) In accordance with the principle of equal treatment of market participants, Art. 102 of the EA establishes a universal obligation for financial liability regarding imbalances.

- **Legal Essence:** Every entity (producer, consumer, or trader) bears direct financial liability for any deviation of its actual production or consumption relative to its registered hourly schedule.

- **Execution Mechanism:** Liability is realized through payments to the Balancing Energy Market Operator (ESO), calculated based on the Methodology for

Determining Balancing Energy Prices approved by the EWRC. Liberalization removes the possibility of offsetting these specific costs by shifting them to other consumer categories.

2.2. The Role of the Aggregator (Art. 96a of the EA) As a risk management tool for small participants (including RES communities and household consumers), pursuant to Art. 96a of the EA, the Independent Aggregator, as a legal entity, pools the loads of multiple end-customers and/or production facilities to operate them as a single portfolio on the energy market.

The primary legal advantage of aggregation is the achievement of internal balancing. By diversifying the profiles of individual members, the aggregator averages out deviations and protects small participants from extreme prices on the balancing market, which would be prohibitive for an individual entity.

2.3. The Conflict: Base-load Capacities vs. RES Communities

Although the law is technologically neutral, the practical application of Art. 102 creates varying intensities of financial risk:

- Predictable Base-load Capacities (NPP, TPP): Due to their high predictability, systemic inertia, and planning capabilities, they rarely generate significant imbalances, providing them with a distinct competitive advantage.

- Stochastic Capacities (RES): Their production depends on meteorological conditions, making them legally vulnerable to the Methodology for Determining Balancing Energy Prices approved by the EWRC. In periods of high deficit or surplus, financial penalties for small communities may exceed their revenues from energy sales. This weather dependency places them in a state of constant imbalance risk. [6]

In a liberalized environment, this necessitates that RES communities enter into contracts for participation in a Balancing Group or utilize the services of an Aggregator, making these contracts a key element of their legal and economic viability. Small RES communities must rely on aggregators (Art. 96a of the EA) to avoid the heavy financial penalties for imbalances that were previously "diluted" within the regulated market.

2.4. Legal Mechanisms for Ensuring Stability (Art. 96a and Art. 103 of the EA)

Under free-market conditions, the protection of participants is realized through strict licensing requirements and the introduction of new operational self-regulation tools.

- The Institute of the "Balancing Group Coordinator": Pursuant to Art. 96a of the EA, the coordinator is an entity licensed for key energy activities (production, transmission, distribution, trade, or aggregation) that cumulatively meets the requirements for financial guarantee of transactions and is registered by the ESO. From a legal standpoint, this requirement functions as a system of shared responsibility: the coordinator

assumes joint and several financial risk for imbalances, guaranteeing systemic sustainability through its solvency.

- Demand Response as a Protective Tool: Although dispatching is subject to market principles, Art. 94a of the EA provides a legal framework for active Demand Response. This is the core mechanism through which small communities and end-customers can minimize their own deviations. By utilizing storage systems (batteries) or consumption flexibility, they transform technical availability into an economic resource, thereby avoiding imbalance penalties.

The regulatory framework (specifically Art. 96a and Art. 102 of the EA) catalyzes the transformation of small communities from passive consumers into active market entities. They are normatively compelled to enter into complex legal and financial relationships with aggregators or coordinators, which represents the only legal path to ensuring their economic survival in a liberalized environment.

The transformation of the energy sector highlights the regulator's role as a guarantor of predictability. Current balancing methodologies penalize energy communities for the stochastic nature of their output, necessitating an urgent revision of pricing mechanisms. Transitioning to capacity-based grid charges will reshape the sector's economic logic. This will act as a direct incentive for investment in local storage systems, which is vital for reducing peak loads. The result would be twofold: fewer technical constraints for baseload generators and a more secure revenue stream for the Security of the Electricity System Fund.

2.5. Collision in the Allocation of Balancing Costs and Financial Liability

The regulatory vacuum regarding Flexible Grid Contracts compels the system operator to employ inefficient measures, such as the suboptimal dispatching of baseload plants like the Kozloduy NPP. The current model of priority access for RES communities - devoid of financial commitments to grid stability - distorts market signals. Transitioning toward market-based dispatch of decentralized resources through aggregators would eliminate the need to socialize balancing costs. Implementing flexibility mechanisms is essential to ending the practice where baseload plants absorb the negative externalities caused by peak production from distributed energy sources.

The primary legal conflict is rooted in the absence of an adequate mechanism for allocating balancing costs. Nuclear capacities operate in a regime of technological inertia. When energy communities generate a sudden surplus, the ESO is obligated by virtue of Art. 73 of the EA to maintain systemic stability, which necessitates the curtailment of capacities.

There is a lack of a legal instrument that assigns financial liability for the operation of a base-load capacity in a non-optimal regime when this is a direct consequence of the priority of RES communities under the ERSA.

Although Art. 93a and Art. 94a of the EA regulate the free energy market and balancing, there is a contradiction with Art. 83, Para. 1. Base-load capacities are forced to violate their approved schedules due to the priority access of RES. Pursuant to Art. 99 of the EA, the ESO organizes the balancing energy market, but the costs from the forced curtailment of base-load plants are not recovered from the initiators of the surplus (the RES communities). This leads to the improper socialization of individual costs within the overall system price.

Despite the introduction of citizen energy communities, the law does not detail their property liability in cases of induced system overloads.

Institutional efforts in the 2024–2026 period have been directed toward liberalization but do not definitively address the structural conflict between base-load and variable capacities:

The amendments to the EA introduced the principle of full financial liability for imbalances for all market participants, including aggregators (Art. 1, Para. 4). Nevertheless, the retention of specific exceptions and derogations for certain entities maintains a state of legal uncertainty and hinders equality in bearing systemic costs. The promulgated Methodology for Calculating Electricity Quantities for Energy Communities represents a technical instrument for net settlement. However, it is of an explicitly administrative nature and does not provide a legal mechanism for the recovery of direct losses of base-load capacities incurred during forced curtailment of their production.

The proposed amendments to the ERSA aim to accelerate administrative procedures for connection. The focus of the legislator remains on the quantitative entry of RES, without the parallel introduction of norms for property liability regarding grid stability or compensatory mechanisms for base-load plant operators.

By 2026, the regulatory framework already identifies the sources of imbalance through the pricing of balancing energy, but a regulatory vacuum remains regarding the guarantees for the financial sustainability of base-load capacities when operating in a non-optimal technical regime.

2.6. Regulatory Uncertainty during "Emergency States"

The legal framework in the EA (Art. 72, 73, 188-191) grants the ESO the right to impose restrictive regimes, yet regulatory uncertainty exists regarding the control over decentralized energy communities during crises. A proposal for a normative solution includes the explicit inclusion of communities under the direct operational control of the ESO, the introduction of a "capacity component" fee (Art. 104), and a mandatory remote control connection (Art. 92b) to prevent risks to national security. The refinement of the term "restrictive regime" and the normative hierarchy is of key importance for the effective management of energy emergencies. [7]

V. CONCLUSIONS

The analysis of the current regulatory framework confirms that although the EA provides a stable foundation for the management of base-load capacities, the legal integration of decentralized production under the ERSA remains in an initial stage. The primary challenge is of a regulatory nature: establishing a normative balance between the technological inertia of nuclear energy and the dynamics of energy communities, without compromising systemic stability and social justice.

Main conclusions:

1. Normative Fragmentation: The EA and ERSA operate under a lack of systemic coordination. The burden of maintaining systemic security is disproportionately distributed upon centralized capacities, while decentralized entities benefit from market preferences, which generates an economic imbalance.
2. Deficit in Capacity Management: The absence of precise rules for grid capacity sharing leads to unjustified restrictions for energy communities in zones with planned development of new nuclear capacities.

Specific recommendations for legislative amendments:

1. Synchronization of Secondary Legislation: Revision of the EWRC Ordinances with the aim of introducing a unified protocol for remote load management, applicable to all categories of producers.
2. Regulation of "Flexible Grid Contracts": Legislative introduction of contractual models in which energy communities receive reduced connection fees in exchange for explicit consent for operational production curtailment during periods of peak load on base-load capacities.
3. Reform of the Tariff Model: Transformation of grid services from volumetric fees (per kWh) to capacity fees (per kW). This will ensure fair participation of communities in the maintenance costs of the grid infrastructure.

The sustainable development of the Bulgarian energy sector depends on a transition from a model of competition to a model of legal symbiosis. The future requires a transformation of the energy grid from passive infrastructure into an intelligent market, regulated through flexible, fair, and technologically neutral legislation. These changes will ensure that energy communities develop as active and responsible partners, rather than as external factors to the system whose benefits are paid for by base-load energy and vulnerable consumers.

REFERENCES

- [1] W. Kuo, *Fiabilité de l'énergie renouvelable et nucléaire*, Iste, ISBN:978-1-78405-054-2, pp. 156-159, 2015;
- [2] L. Moreno, D. Abaunza, T. Rodríguez, *Formación de un derecho de la transición energética*, Universidad Externado de Colombia, ISBN: 9786287620841, pp. 83-97, 2023;
- [3] A. Alonso, *El multicolor de la energía. Desafíos y oportunidades para la transición energética*, Universidad Autónoma Metropolitana y Fundación Rosa Luxemburg, ISBN: 607-28-3093-6, pp. 34-48, 2024;

[4] O. Gamel, *Énergie citoyenne, synergie locale*, Sciences PoLyon, ISBN: 978-2-491924-59-1, pp. 27-35, 2025;
[5] L. Freris, D. Infield, *Les Energies renouvelables pour la production d'électricité*, EAN: 9782100824540, pp. 237-248, Dunod, 2021;
[6] N. Jelly, *Les énergies renouvelables*, Chrono Sciences, EAN: 9782987526902, pp. 45-63, 2022;

[7] A. Boute, *Energy Dependence and supply security: Energy Law in the New Geopolitical Reality*, Oxford University Press, ISBN:9780198890515, pp. 27-39, 2023;

Legal Transformation of the Bulgarian Energy Sector: From a Centralized Model to a Decentralized Regulatory Framework for Renewable Energy Sources and Renewable Energy Communities

Olga Borisova

Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
olga.borisova@vfu.bg

Abstract— This report analyzes the fundamental regulatory transformation of the Bulgarian energy sector, stemming from the transition from the traditional centralized model to a decentralized legal framework for renewable energy sources. The primary research focus is directed toward the conceptual alignment and existing contradictions between the Energy Act and the Energy from Renewable Sources Act. Despite the introduction of progressive European definitions such as "active consumer" and "renewable energy community," the analysis identifies a significant regulatory dualism that hinders the actual functionality of these new market entities.

The study identifies key barriers to energy decentralization arising from the conservative architecture of the Energy Act and the lack of applied methodology in secondary legislation. Special attention is paid to the need for reform in the licensing regimes of the Energy and Water Regulatory Commission and the introduction of differentiated "local grid fees" to reflect the actual load on the grid during production and consumption within a single community.

The scientific contribution of the report is expressed in the formulation of specific proposals for legislative amendments, including the creation of a "one-stop-shop" digital register at the Sustainable Energy Development Agency to eliminate administrative duplication. The author substantiates the conclusion that without urgent regulatory corrections, energy decentralization in the Republic of Bulgaria will remain in a state of functional inefficiency, blocking strategic goals for a sustainable energy transition and decarbonization.

Keywords— Decentralization, Energy transition, Legislative amendments, Renewable energy.

I. INTRODUCTION

The energy sector is undergoing a fundamental regulatory and structural transformation—a transition from a centralized, vertically integrated model toward a decentralized, low-carbon system. In the Republic of Bulgaria, this process represents a complex regulatory challenge, shaped by the country's commitments under European Union law and the strategic objectives of the "European Green Deal."

The subject of this report is the legal reconfiguration of the Bulgarian energy market, determined by the "Clean Energy for all Europeans" legislative package. The study focuses on the interference between established administrative practice and the legal status of new entities: active customers and energy communities.

Traditionally, the Bulgarian legal framework defined the end-user as a passive subject—a recipient of a service of public interest. Through the transposition of Directive (EU) 2018/2001 [1] and Directive (EU) 2019/944 [2] into national legislation (the Energy Act and the Energy from Renewable Sources Act), the foundations of a new regulatory model have been established. [3] Its goal is to provide households and small businesses with the regulatory instruments necessary for active participation in market mechanisms and energy resource management.

The central thesis of this report is that while the national regulatory framework has been formally aligned with the principles of decentralization, there are systemic deficits in

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.25>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

the implementing regulations. The identified contradictions necessitate urgent legislative synchronization to transform decentralization from a legal declaration into an effectively functioning market mechanism. Within this report, these deficits will be analyzed through the prism of current law, and specific guidelines for legislative optimization will be proposed.

II. MATERIALS AND METHODS

The methodology of this research is predicated on a multidimensional legal analysis designed to evaluate the effectiveness of the Bulgarian regulatory framework in the context of energy decentralization. The study employs a combination of qualitative research methods to assess the alignment between national legislation and European Union mandates.

The primary "materials" of this study consist of an extensive corpus of primary and secondary legal acts, structured into three hierarchical levels:

- **European Supranational Framework:** Analysis of Directive (EU) 2018/2001 (RED II), Directive (EU) 2019/944, and Directive (EU) 2023/2413 (RED III) [4], which serve as the normative benchmark for decentralization.
- **National Primary Legislation:** Evaluation of the Energy Act (EA) [5] and the Energy from Renewable Sources Act (ERAS) [6], focusing on the provisions defining "active customers," "renewable energy communities," and "citizen energy communities".
- **Secondary Legislation and Administrative Norms:** Examination of Ordinance No. 6 of March 28, 2024, on the Connection of Facilities to Electricity Networks, and the Rules for Electricity Trading. [7]
To achieve the research objectives, the following scientific methods were applied:
- **Formal-Dogmatic Method:** Used to interpret the literal meaning and legal scope of specific definitions, such as the "urbanized territory" requirement for renewable energy communities and the legal status of the "active customer".
- **Comparative Legal Analysis:** Employed to identify the gaps between the idealized European models of "energy democracy" and their technical transposition into Bulgarian law. This method highlights the discrepancies between the promotional regime of the ERAS and the restrictive administrative architecture of the Energy Act.
- **Systemic-Structural Analysis:** Applied to examine the horizontal and vertical relationships between market participants (distribution system operators, regulators, and communities). This approach was crucial for identifying the "regulatory dualism" where overlapping jurisdictions of Sustainable Energy Development Agency (SEDA) and Energy and Water Regulatory Commission (EWRC) create administrative barriers.
- **Teleological Interpretation:** Used to evaluate whether the current secondary legislation (such as the lack

of virtual net metering mechanisms) aligns with the ultimate goals of the "European Green Deal" - namely decarbonization and citizen empowerment.

The study followed a three-stage analytical process:

1. **Identification of Normative Inconsistencies:** Mapping the contradictions between the EA and the ERAS regarding entity registration and market participation.
2. **Functional Assessment:** Analyzing the practical operability of "energy sharing" under the existing electricity trading rules.
3. **Synthesis and Proposal:** Formulating *de lege ferenda* proposals for legislative optimization, including the creation of a "one-stop-shop" registry and the introduction of differentiated grid fees.

III. RESULTS AND DISCUSSION

1. EU LEGAL FRAMEWORK IN THE FIELD OF DECENTRALIZED ENERGY

1.1. Retrospective Review of EU Primary and Secondary Law: Transition Toward Decentralized Energy Models (RED I, II, III)

The evolution of European law in the renewable energy sources (RES) sector marks a transition from the centralized planning of state capacities toward the decentralized empowerment of the individual market participant. [8]

Within the framework of modern energy transformation, the shift toward a decentralized operational model fundamentally alters the legal status of the consumer—moving from a passive recipient of a service to an active market participant. This concept is closely linked to the liberalization of the electricity sector and the implementation of Smart Grids, which allow entities to simultaneously consume and produce energy.

A retrospective legal analysis reveals that until the late 1990s, there was no comprehensive or binding EU legal framework for the RES sector. The process of codification began gradually, culminating in successive amendments to the Renewable Energy Directive (known as RED I, RED II, and the current RED III), which institutionalized the rights of energy communities and energy-sharing mechanisms. [9]

During this period, energy policy was viewed primarily as a prerogative of national sovereignty rather than an object of unified EU legislation. Technologically and economically, the renewable energy sector (wind and solar) was characterized by high capital intensity and treated as "experimental" compared to conventional capacities (coal and nuclear).

The legal regulation of the sector entered a new stage in 2001 with the adoption of Directive 2001/77/EC [10], which introduced the first specific targets for promoting electricity from renewable sources within the internal market. It set a general indicative target of a 21% share of RES in the Community's gross electricity consumption by 2010. [11]

In 2009, Directive 2009/28/EC (RED I) [12] established the first comprehensive legal framework, extending the scope of regulations to the heating, cooling, and transport sectors. This early stage institutionalized the RES sector through mandatory national targets. In Bulgaria, this led to a boom in large-scale photovoltaic and wind farms, but within a strictly centralized model. The legal framework treated RES capacities as industrial facilities, without providing a role for the small-scale consumer.

The subsequent revision took place in 2018 via Directive (EU) 2018/2001 (RED II), which codified the rules for the period up to 2030. This directive effected a radical legal shift by defining "energy democracy." It mandated that Member States recognize the right of citizens to be "active consumers". A key contribution was the legalization of energy communities, which were granted the right to produce, consume, and share energy within closed or local structures. [13]

Currently, this framework has been substantially amended and enhanced by Directive (EU) 2023/2413 (RED III). It accelerates decentralization by introducing the concept of "overriding public interest" in the construction of RES and aims to remove administrative barriers through "renewables acceleration areas" (RAAs), designed to overcome the inertia of local legislation.

1.2. Transformation of the Legal Status of Consumers: Evolution of the Decentralized Model in RED II and RED III

Directive (EU) 2018/2001 (RED II) and its subsequent amendment via Directive (EU) 2023/2413 (RED III) introduce fundamental changes to the structure of the energy market, institutionalizing the model of decentralization.

The regulatory framework places new legal entities at its center—active customers, energy communities, and independent aggregators—which are key to the integration of RES capacities and the management of system flexibility.

Under the new regulations, end-customers transform their status from passive consumers into active participants with the right to produce, store, and trade electricity. This model delegates management to the local level, granting energy communities and local authorities autonomy in managing their own energy resources.

In this context, ensuring system stability becomes a shared responsibility. The regulatory framework must guarantee non-discriminatory grid access by eliminating unjustified administrative barriers for small-scale producers and facilitating their inclusion in market balancing mechanisms.

A critical element in the new regulatory architecture is the concept of "energy sharing," which allows active customers to distribute energy produced from collective renewable capacities among themselves without being subject to excessive grid fees or complex administrative procedures. RED III mandates that Member States remove

obstacles to this mechanism, ensuring it is also accessible to low-income households.

Consequently, decentralization is not only a technological tool but also a socio-economic instrument. By fostering energy communities, the legislation aims to combat energy poverty by providing vulnerable consumers with direct access to cheaper, locally produced energy. In this way, the energy transition is transformed into an inclusive process where the benefits of decarbonization are distributed fairly, and regulatory bodies assume the role of guarantors for social cohesion and consumer protection within a dynamic market.

2. REGULATORY REGIME OF DECENTRALIZATION: STRUCTURAL AND FUNCTIONAL CHARACTERISTICS OF THE REGULATORY MODEL

The decentralized model is not merely a technical distribution of capacities, but a new legal architecture that reshapes the hierarchical relationships between the regulator, operators, and consumers. Its specificities manifest in three primary areas:

2.1. Horizontal Legal Relations and "Network Neutrality"

Traditional vertical "state monopoly–customer" relationships are being replaced by horizontal contracts and a transformation of the network operator's role from a "trader" into a "neutral facilitator." Its legal role is to ensure non-discriminatory grid access for a multitude of small participants, guaranteeing technical safety without imposing economic barriers. The process of integrating energy from renewable sources necessitates a transformation of the market structure, replacing the traditional hierarchical system with a model based on decentralized production capacities and local consumption. The normative recognition of the status of "active customers" and "energy communities" redefines the functions of network operators. Within this framework, digitalization and Smart Grids are established as imperative technological and legal instruments for ensuring system balance at the local level.

According to Directive (EU) 2018/2001 (RED II) and Directive (EU) 2019/944, which define the decentralization model, the legal structure of the decentralized model is based on two main types of entities: renewable energy communities and citizen energy communities.

2.2. Institutionalization of "Flexibility" as a Legal Object and the Localization of Legal Regulation

The decentralized model introduces flexibility (the ability to adjust consumption/production in real-time) as a commodity with legal value.

- **Balancing Services:** The legal framework must allow small entities (via aggregators) to participate in the balancing energy market. This requires new types of standardized contracts and a refinement of balancing responsibility, which in the centralized model was borne by a few large power plants.

This model is characterized by increased resilience, yet simultaneously entails higher administrative and technical complexity. This necessitates the implementation of a dynamic regulatory framework capable of adapting to the intermittency of production and real-time changes in grid load.

2.3. Decentralization of Market Management

The state regulatory body is ceasing the practice of directive planning regarding production volumes and is moving toward establishing a market framework that guarantees small-scale producers the right to freely sell surplus energy. The functioning of this model is predicated on the normative introduction of Smart Metering systems, which allow for real-time accounting. It is imperative to integrate dynamic electricity tariffs that reflect price fluctuations on organized exchange markets on an hourly basis, aiming to provide price incentives for consumers to optimize their load profiles during periods of RES overproduction.

3. TRANSPOSITION AND ADAPTATION OF EU LAW INTO THE NATIONAL FRAMEWORK: ANALYSIS OF AMENDMENTS TO THE ERAS

3.1. Legal Regime and Subject Composition of Decentralized Production under the ERAS

The legal framework for decentralization in Bulgaria is structured around three main pillars within the Energy from Renewable Sources Act, which regulate the status of new participants and their scope of competence.

3.1.1. Active Customer (Art. 18a of the ERAS) The legislator regulates the status of the "end-customer as an active customer," granting them the right to produce energy for their own consumption, to store it, and to sell the surplus on the market.

Pursuant to § 1, item 59 of the Additional Provisions of the ERAS Act, this is an entity operating on its own property for whom energy production is not a primary commercial activity (applicable to non-household consumers).

Provisions under Art. 18a, para. 1–4 guarantee the right to participate in support schemes and energy markets without the entity losing its status as an end-customer.

3.1.2. Renewable Energy Community (Art. 18b of the ERAS Act):

The legislator regulates collective participation in the energy transition through the figure of the "Renewable Energy Community" (REC). It functions as an autonomous entity uniting local resources and consumers.

Legal Definition (§ 1, item 56 of the AP of the ERAS): An REC is an entity based on open and voluntary participation; it is independent and effectively controlled by its shareholders, partners, or members (natural persons, SMEs, or municipalities). The definition requires the community to own and manage RES installations and consumption sites located within an urbanized area.

The primary objective of an REC is to provide environmental, economic, or social benefits to the local community rather than generating financial profit. The entity may take any legal-organizational form, provided it meets the criteria for independence and control.

Pursuant to Art. 18b, para. 2, the community has a legally recognized right to:

- Produce, consume, store, and sell energy from renewable sources;
- Share produced energy among its members while maintaining their rights as end-customers;
- Access all energy markets directly or through aggregation.

The requirements of Art. 92b of the Energy Act apply accordingly to renewable energy communities.

3.1.3. Citizen Energy Community (Art. 92 et seq. of the Energy Act)

The ERAS does not contain a separate regulatory framework for Citizen Energy Communities (CECs), as they are entities of the general electricity market, whereas the ERAS Act specifically regulates Renewable Energy Communities (RECs).

A "Citizen Energy Community" is a legal entity whose regulation is integrated into the general framework of the electricity market via the Energy Act.

Legal Definition (§ 1, item 76 of the AP of the Energy Act): A CEC is a legal entity that:

- a) is based on voluntary and open participation and is effectively controlled by members, partners, or shareholders who are natural persons, local authorities (municipalities), or small enterprises;
- b) has as its primary purpose the provision of environmental, economic, or social community benefits for its members or shareholders or for the local areas where it operates, rather than financial profits; and
- c) may engage in generation, including from renewable sources, distribution, supply, consumption, aggregation, energy storage, energy efficiency services, or charging services for electric vehicles, or provide other energy services to its members or shareholders.

The regulation of the Citizen Energy Community in Bulgarian legislation was introduced through references to the European framework; however, at present, the core operational rights of CECs in the Energy Act are systematized in Art. 4, para. 2, item 21 (as part of state policy) and detailed in Art. 92 et seq. concerning the free market and aggregation. [14]

In general, the organizational rights of a CEC are:

Energy Sharing: The community has the right to organize the sharing of electricity generated from its production facilities, ensuring that the rights of its members as end-customers are maintained.

Cooperation with Operators: Grid operators are obliged to cooperate with CECs to facilitate energy transfers within the community under non-discriminatory conditions.

Unlike an REC, a CEC is not restricted by a requirement for "urbanized territory."

A CEC can operate with any type of electricity, whereas an REC is strictly limited to renewable energy sources.

4. ADMINISTRATIVE AND LEGAL REGIME FOR GRID CONNECTION WITHIN THE PROCEDURAL FRAMEWORK ACCORDING TO ORDINANCE NO. 6 OF MARCH 28, 2024

With the entry into force of the new Ordinance No. 6 of March 28, 2024, on the Connection of Facilities to Electricity Networks, the administrative burden on energy communities has been significantly reduced through the introduction of the following preferential conditions and procedural reliefs:

4.1. Accelerated and Simplified Procedural Framework for Connection (Art. 2, para. 7)

The new ordinance allows the feasibility study of connection conditions for RES production facilities (including those owned by communities) to be conducted under the simplified procedure of Art. 22 of the ERAS. This includes:

- Shortened deadlines for the issuance of opinions by network operators.
- Notification-based connection for small-scale installations that are part of the consumption facilities of community members.

4.2. Legal Qualification and Connection of Facilities in "Internal Installation" Mode (Art. 4, para. 1)

Pursuant to Art. 4, para. 1, when a community builds an installation connected to an existing consumption facility (e.g., on the roof of an administrative building or a residential block), it is treated as part of the already connected facility. This eliminates the need to open an entirely new customer account and avoids cumulative administrative requirements for establishing a new point of connection.

4.3. Guaranteed Non-discrimination (Art. 3, para. 2)

According to the ordinance, network operators may refuse the connection of energy community facilities only in cases of a proven threat to the security of the energy system or the quality of supply.

4.4. Commissioning and Temporary Schemes (Art. 2, para. 8)

The ordinance provides the possibility for energy transmission immediately following commissioning under the Spatial Planning Act, including under temporary access schemes, which allows for a faster start to energy-sharing activities.

4.5. Licensing Reliefs (Art. 10, para. 3 and para. 5)

Within the framework of a closed electricity distribution network (e.g., in industrial zones or complexes), the licensing regime is relaxed, allowing for the issuance of a

license for energy facilities with integrated activities spanning one or more land plots.

The presented analysis outlines three levels of decentralization in the Bulgarian energy sector, which transform the end-customer from a passive consumer into an active market participant.

The main conclusions are as follows:

- The Active Customer (Art. 18a of the ERAS Act) represents the most accessible form of decentralization, focusing on individual energy independence and the right to self-generation and storage.
- The Renewable Energy Community (Art. 18b of the ERAS Act) is a strictly defined entity for the local self-management of green energy, limited by requirements for geographical proximity and the placement of assets within urbanized territories.
- The Citizen Energy Community (Art. 4, para. 2, item 21 and the AP of the Energy Act) constitutes the broadest framework for collective participation; it is technologically neutral and allows for the integration of diverse energy services (such as aggregation and EV charging) without territorial restrictions.
- The new Ordinance No. 6 of 2024 completes this legal framework by providing the necessary administrative reliefs and shortened connection procedures. In this manner, the legislator not only legitimizes these new entities but also creates practical mechanisms for their operation, guaranteeing non-discriminatory access to both the grid and the market.

IV. CONCLUSION

Alongside the progress achieved, an objective normative inconsistency is observed, arising from the lack of conceptual synchronization between the Energy Act and the Energy from Renewable Sources Act.

While the EA regulates the macro-structural framework and centralized management with a view toward security of supply, the ERAS introduces a decentralized functional model based on horizontal connectivity and the autonomy of local energy resources.

4.1. Systemic Deficiencies of the Current Legal Framework:

4.1.1. Procedural Inconsistency for Entities with Hybrid Legal Status: When a Citizen Energy Community operates exclusively with renewable energy assets, it falls under the scope of cumulative application of the general market regime (under the EA) and the promotion regime (under the ERAS). The lack of a unified administrative procedure creates an unjustifiably high barrier to market entry. The entity is placed in a position where it must prove resource adequacy according to criteria applicable to large commercial companies, which neutralizes the preferences provided in the ERAS for socially oriented structures.

4.1.2. Conflict Between Territorial Determinacy and Technological Applicability: A conceptual conflict is identified between the restrictive requirement for

"urbanized territory" (§ 1, item 56 of the AP of the ERAS) and the possibility of locating RES capacities on agricultural land or outside the boundaries of settlements. This requirement places communities in a state of institutional disintegration: they possess the subjective right to generate energy but are deprived of their preferential legal regime solely on the basis of the territorial location of their production assets.

4.1.3. Lack of Secondary Legislation Methodology for "Energy Sharing"

Although the ERAS Act and the Energy Act legitimize the right to share energy, the Ordinance on Electricity Price Regulation and the Measurement Rules lack a defined mechanism for so-called virtual net metering. This renders the right to share a "hollow norm," as network operators have no legal obligation (or technical procedure) to perform the clearing and settlement of shared volumes between the individual customer accounts of members.

4.1.4. Regulatory Duplication of Oversight

The requirement for simultaneous registration in the registries of both the Sustainable Energy Development Agency and the Energy and Water Regulatory Commission, accompanied by differing reporting criteria, creates unnecessary administrative pressure. This leads to a regulatory gap regarding the protection of small communities, which are treated as professional market participants without possessing their commercial capacity.

These systemic contradictions necessitate urgent legislative synchronization to transform decentralization from a legal declaration into a functional market mechanism. [15]

4.2. Guidelines for Regulatory Alignment and Legislative Amendments

To achieve full operability of the subjective rights of energy communities and active customers, a subsequent normative consolidation is required in the following areas:

4.2.1. Amendments to the Electricity Trading Rules:

Regulation of "Virtual Net Metering": Introduction of a detailed clearing methodology, whereby the energy produced by the community is proportionally deducted from the individual consumption of its members within the same billing period.

Status of "Internal Supplier": Recognition of the right of communities to perform internal distribution and settlement without requiring an "electricity trader" license, provided the activity is restricted to the members of the community.

4.2.2. Refinement of Ordinance No. 6 of 2024 on Grid Connection:

Unified Notification Regime: Standardizing procedures for RECs and CECs by removing the "urbanized territory" requirement as a condition for simplified connection when the capacity is below 100 kW.

Obligation for "Dynamic Grid Management": Distribution System Operators should be mandated to provide real-time data regarding available connection capacity across grid branches to facilitate the planning of community projects.

4.2.3. Amendments to the Ordinance on Electricity Price Regulation:

Differentiated Grid Fees: Introduction of "local grid fees" for energy produced and consumed within the same community (low voltage), reflecting the fact that this energy does not burden the transmission network or medium-voltage transformers.

4.2.4. Creation of a "One-Stop Shop" Registry at SEDA:

Centralized Administration: Merging the registration regimes of SEDA and EWRC for small energy communities into a single digital portal. This will eliminate regulatory duplication and reduce administrative costs for these entities.

In the absence of the aforementioned regulatory corrections, energy decentralization in Bulgaria will remain in a state of functional inefficiency. Such a scenario leads to the blocking of the legitimate objectives of the ERAS Act by the conservative legal architecture of the Energy Act and the lack of an applied methodology in the secondary legislation.

REFERENCES

- [1] Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources [Online], Available: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32018L2001> [Accessed: May 6, 2026];
- [2] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [Online], Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0944> [Accessed: May 6, 2026];
- [3] M. Roggenkamp, K. Graaf, R. Fleming, *Energy Law, Climate Change and the Environment*, Publisher: Edward Elgar, ISBN: 9791788119672, pp. 623-639, 2021;
- [4] Directive (EU) 2023/2413 of the European Parliament and of the Council of 18 October 2023 amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652 [Online], Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023L2413> [Accessed: May 6, 2026];
- [5] Energy Act [Online], Available: <https://lex.bg/bg/laws/ldoc/2135475623> [Accessed: May 6, 2026];
- [6] Energy from Renewable Sources Act [Online], Available: <https://lex.bg/bg/laws/ldoc/2135728864> [Accessed: May 6, 2026];
- [7] Ordinance No. 6 of March 28, 2024, on the Connection of Facilities to Electricity Networks [Online], Available: <https://lex.bg/bg/laws/ldoc/2137241702> [Accessed: May 6, 2026];
- [8] F. Sales, *Energía Renovable: La dirección correcta para un mundo sostenible*, ISBN: 979-8859944514, 2023;
- [9] C. Acket, J. Vaillant, E. Technip, *Energie renouvelable. Etat des lieux et perspectives*, ISBN: 9782710811756, pp. 58-73, 2016;

- [10] Directive 2001/77/EC of the European Parliament and of the Council of 27 September 2001 on the promotion of electricity produced from renewable energy sources in the internal electricity market [Online], Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0077> [Accessed: May 6, 2026];
- [11] O. Wooley, Renewable Energy Law, Bloomsbury Publishing, ISBN: 9781509936465, pp. 201-232, 2023;
- [12] Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing Directives 2001/77/EC and 2003/30/EC [Online], Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32009L0028> [Accessed: May 6, 2026];
- [13] R. Carlos Torres Flores, La Hora de la Transición energética. Exigencias del Nuevo paradigma: sustentabilidad, seguridad e igualdad, Libros Grano de Sal, ISBN: 9786073050227, pp. 127-136, 2021;
- [14] K. Talus, Introduction to EU Energy Law, OUP-Oxford University Press, ISBN: 9780198791829, pp. 42-48, 2016;
- [15] K. Neri, Le droit international el le nucléaire, Bruylant, EAN: 9782802768517, pp. 273-284, 2021

Secure and Resilient Operation of Hybrid PV-Wind-Storage Systems for Modular E-Fuel Production under Disturbances

Iliyan Hutoy
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
i.hutoy@di.mod.bg

Petia Nedyalkova
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
<https://orcid.org/0009-0006-7156-0891>

Hristo Hristov
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
h.hristov@di.mod.bg

Abstract—Secure and resilient operation is a critical requirement for modular Power-to-Liquid e-fuel plants supplied by intermittent renewable energy. This paper investigates a modular e-fuel production architecture powered by a hybrid photovoltaic-wind-battery system and evaluates its response to short-duration renewable disturbances. A deterministic operational model is formulated for renewable generation, battery buffering, electrolyzer dispatch, hydrogen production, and aggregate fuel synthesis. To improve engineering realism, the framework incorporates electrolyzer ramp-rate constraints and a degradation-aware operating index. The optimization objective is to sustain fuel continuity while limiting curtailment, electrolyzer power variance, and dynamic stress. Beyond the main stressed-case comparison, the study includes sensitivity analysis of the PV/Wind ratio and storage capacity, together with Monte Carlo uncertainty analysis under stochastic renewable fluctuations. Relative to the no-buffer baseline, the optimized dispatch increases daily fuel output by 11.6%, reduces electrolyzer power variance by 66.3%, and improves the disturbance-window resilience score by 36.2%. The results show that secure operation of modular PtL plants emerges from coordinated design of renewable mix, storage, and supervisory control rather than from renewable-following logic alone.

Keywords—deterministic optimization, hybrid PV-wind-storage system, modular e-fuel production, resilient operation.

I. INTRODUCTION

Power-to-Liquid (PtL) technology is increasingly regarded as a practical pathway for producing low-carbon synthetic fuels for aviation, maritime transport, and other hard-to-electrify sectors [4], [10]–[12]. Yet the viability of modular e-fuel plants depends not only on the nominal efficiency of chemical conversion, but also on the secure

and resilient operation of the upstream energy-supply system. In hybrid renewable architectures, photovoltaic generation, wind generation, battery storage, and electrolyzer dispatch are strongly coupled in time, so renewable intermittency can propagate into instability, curtailment, reduced fuel continuity, and increased component stress [9], [13]–[15].

This challenge is especially relevant for modular industrial concepts inspired by current INERATEC-type deployments, where plant operation must remain robust under fluctuating renewable input and short-duration disturbances [2], [3]. In such systems, operational security is not a peripheral issue; it is a systems-design problem. Resilience, system stability, and disturbance handling must therefore be treated as explicit engineering objectives rather than secondary performance outcomes [1], [9].

Against this background, the present paper studies the secure and resilient operation of a hybrid PV-wind-storage system supplying a modular e-fuel plant under disturbances. The contribution is fourfold. First, it formulates a deterministic plant-operation model and the associated supervisory optimization problem. Second, it quantifies the operational benefit of the optimized strategy using explicit performance metrics. Third, it evaluates design sensitivity with respect to the PV/Wind ratio and storage capacity, and tests robustness through Monte Carlo uncertainty analysis. Fourth, it adds engineering realism by introducing electrolyzer ramp-rate constraints and a compact degradation-aware operating model. Throughout the manuscript, industrial ERA ONE values are treated as literature-reported benchmark data, while the fuel-output, resilience, curtailment, and degradation-related metrics are simulated or derived quantities generated by the reduced-order supervisory model. The resulting framework is

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.180>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

closely aligned with the conference themes of secure systems design, system stability, disturbance handling, and sustainable energy technology development.

II. OPERATIONAL FRAMING FOR SECURE AND RESILIENT PTL SYSTEMS

The target plant is represented by six coupled subsystems: photovoltaic generation, wind generation, battery storage, a proton-exchange-membrane electrolyzer, a hydrogen buffer, and an aggregate fuel-synthesis block. The scope is operational rather than reactor-level. The hydrogen buffer is included conceptually as an intermediate continuity element between electrolysis and aggregate fuel synthesis; in the present reduced-order formulation, it is not resolved by a full state-space mass-balance model and is therefore not assigned a separately optimized storage trajectory. Instead, its role is reflected indirectly through the continuity objective and the disturbance-resilience interpretation. The model does not attempt catalyst-scale chemistry or CFD; instead, it captures the cross-couplings that determine plant-level resilience, stability, and fuel output under intermittent renewable supply.

From an operational systems viewpoint, resilience is not a property of a single component. It emerges from the coordinated behavior of the photovoltaic, wind, storage, and electrolyzer subsystems during shortages and surpluses. In this study, system stability is represented by low electrolyzer-power variance and reduced dynamic stress, while disturbance handling is represented by output retention during a forced one-hour renewable shortfall. This framing keeps the paper closely aligned with secure systems design in its engineering sense.

III. OPERATIONAL MODEL AND DETERMINISTIC OPTIMIZATION

The operational simulation horizon is 24 h with a 5 min time step. Renewable input is generated from a daytime photovoltaic profile and a non-zero wind profile in order to represent the hybrid PV-wind supply of the modular plant. Because no site-specific measured renewable traces are used in the numerical examples, these profiles are treated as benchmark stress-test signals rather than as production forecasts. The same supervisory model is written so that measured SCADA data, meteorological measurements, or reanalysis-derived irradiance and wind-speed time series can replace the synthetic profiles without changing the control problem. In a measured-profile implementation, PV power should be computed from plane-of-array irradiance and module temperature, while wind power should be mapped from hub-height wind speed through the turbine power curve before applying the same battery, electrolyzer, and hydrogen-buffer constraints. The battery model includes both an energy-capacity constraint and symmetric charge/discharge power limits of 0.40 MW, which prevents unrealistically large short-term buffering actions. The aggregate renewable power before auxiliary-load subtraction is defined as follows:

$$P_{RES}(t) = P_{PV}(t) + P_W(t) \quad (1)$$

where P_{RES} is the aggregate renewable power, P_{PV} and P_W are photovoltaic and wind power

After subtracting the auxiliary load, the remaining power can be directed to the electrolyzer, battery charging, or curtailment. With positive battery power defined as discharge, the power balance is

$$P_{RES}(t) + P_{BAT}(t) = P_{EL}(t) + P_{AUX} + P_{CURT}(t) \quad (2)$$

where P_{BAT} is battery power, P_{EL} is electrolyzer power, P_{AUX} is auxiliary load, P_{CURT} is curtailed power,

The battery state evolves according to a charge/discharge efficiency model, where $SOC(t)$ is the battery state of charge at time step t , expressed as a normalized value or percentage of the rated battery capacity. $SOC(t+1)$ is the battery state of charge at the next time step. $P_{CH}(t)$ is the battery charging power at time t , $P_{DIS}(t)$ is the battery discharging power at time t , η_{ch} is the charging efficiency, and η_{dis} is the discharging efficiency. Δt is the simulation time step, and E_{BAT} is the rated battery energy capacity.

$$SOC(t+1) = SOC(t) + \frac{\left[\eta_{ch} P_{CH}(t) - \frac{P_{DIS}(t)}{\eta_{dis}} \right] \Delta t}{E_{BAT}} \quad (3)$$

The first term inside the brackets increases the state of charge during charging, while the second term decreases the state of charge during discharging. The division by E_{BAT} converts the exchanged energy into a normalized change of battery state of charge.

Hydrogen production is approximated by a power-proportional relationship. At this supervisory level, the downstream fuel-synthesis block is intentionally aggregated rather than reactor-resolved where $\dot{m}_{H_2}(t)$ is the hydrogen produced by the electrolyzer during time step t , η_{EL} is the electrolyzer efficiency, $P_{EL}(t)$ is the electrical power supplied to the electrolyzer at time t , Δt is the simulation time step, and LHV_{H_2} is the lower heating value of hydrogen. The numerator $\eta_{EL} P_{EL}(t) \Delta t$ represents the useful energy converted into hydrogen, while division by LHV_{H_2} converts this energy into an equivalent hydrogen mass.

$$\dot{m}_{H_2}(t) = \frac{\eta_{EL} P_{EL}(t) \Delta t}{LHV_{H_2}} \quad (4)$$

and aggregate synthetic-fuel output is represented by a simplified conversion relationship. This mapping is used only to compare dispatch strategies under common assumptions and should not be interpreted as a detailed process model or direct plant-validation equation.

$$m_{FUEL}(t) = k_{FT} \dot{m}_{H_2} FT(t) \quad (5)$$

where $m_{FUEL}(t)$ denotes the synthetic-fuel mass produced during time step t , $\dot{m}_{H_2}$, $FT(t)$ is the hydrogen mass directed to the aggregate Fischer–Tropsch synthesis block, and k_{FT} is the simplified hydrogen-to-fuel conversion coefficient. This coefficient is used as a reduced-order representation of the downstream synthesis process and is intended for comparative dispatch analysis rather than detailed reactor-level modelling.

The deterministic supervisory objective penalizes renewable curtailment and aggressive stack motion, rewards smooth fuel production, and includes a normalized fuel-output term. Tildes denote normalized quantities used only for weighting and numerical conditioning where J denotes the supervisory optimization objective, P_{CURT} is the curtailed renewable power, ΔP_{EL} is the electrolyzer power change between consecutive time steps, m_{FUEL} is the produced synthetic-fuel mass, m_{REF} is the reference fuel-production trajectory, and $w1$ - $w4$ are weighting coefficients. The first term penalizes renewable curtailment, the second term penalizes aggressive electrolyzer ramping, the third term penalizes deviation from the desired fuel-production trajectory, and the fourth term rewards total synthetic-fuel production:

$$J = w1 \sum P_{CURT} + w2 \sum (\Delta P_{EL})^2 + w3 \sum (m_{FUEL} - m_{REF})^2 - w4 \sum m_{FUEL} \quad (6)$$

The optimization is subject to the operating-envelope constraints, where $u(t)$ is the electrolyzer on/off state and the battery energy and power remain within rated limits and $P_{EL}(t)$ denotes the electrolyzer power at time step t , P_{min} and P_{max} define the allowable electrolyzer operating range, $SOC(t)$ is the normalized battery state of charge, and $P_{CURT}(t)$ is the curtailed renewable power. These constraints ensure that the electrolyzer remains within its stable operating envelope, the battery does not exceed its energy limits, and renewable curtailment is treated as a non-negative surplus-power variable:

$$P_{min} \leq P_{EL}(t) \leq P_{max}, 0 \leq SOC(t) \leq 1, P_{CURT}(t) \geq 0 \quad (7)$$

and, for engineering realism, an explicit ramp-rate limit

$$|P_{EL}(t) - P_{EL}(t-1)| \leq R_{max} \Delta t \quad (8)$$

where $P_{EL}(t)$ denotes the electrolyzer power at the current time step, $P_{EL}(t-1)$ is the electrolyzer power at the previous time step, $R_{max} \Delta t$ is the maximum allowable ramp rate of the electrolyzer, and Δt is the simulation time step. This constraint prevents unrealistically fast set-point changes and keeps the electrolyzer trajectory compatible with stack and balance-of-plant dynamic limitations.

Equation (8) is important because, without it, a controller may exploit the battery as an ideal actuator and command unrealistic stack transitions. By enforcing a maximum set-point gradient, the dispatch remains more compatible with actual balance-of-plant hardware and stack dynamics, which is consistent with recent experimental and review-based evidence for dynamic water-electrolysis systems [5]–[8].

The optimization was implemented as a deterministic reduced-order supervisory-control problem solved over 288 time steps per day. The decision variables are the electrolyzer power trajectory $P_{EL}(t)$ and the battery charge/discharge schedule. The main constraints are the electrolyzer operating window, the battery state-of-charge bounds, the battery power limit, non-negative curtailment, and the electrolyzer ramp-rate limit. A constrained

sequential quadratic programming routine was used in the reference implementation. The stopping rule was a relative objective-function change below 10^{-6} or a maximum of 200 iterations. For the nominal and stressed cases reported here, convergence was typically reached within 20–35 iterations, with wall-clock runtimes below 0.5 s per 24 h case on a standard laptop-class processor.

All objective-function terms were normalized before weighting in order to keep the optimization numerically well-conditioned and to make the design priorities explicit. Curtailment was normalized by a daily curtailment reference scale, the ramp-smoothness term by the baseline sum of squared power steps, the fuel-continuity term by the baseline deviation from the reference production trajectory, and the fuel-maximization term by baseline daily fuel output. Unless otherwise stated, the reported cases use unit weights after normalization for the comparative terms in (6); therefore, the weights represent scheduling priorities rather than physically measurable plant constants.

TABLE I. MAIN MODEL PARAMETERS AND OPERATING LIMITS

Item	Value/ definition	Role in the model
Decision variables	$P_{EL}(t)$, battery charge/discharge schedule	Supervisory control trajectories
Time discretization	24 h horizon, 5 min step, 288 intervals	Deterministic operating horizon
Solver	Sequential quadratic programming	Constrained nonlinear optimization
Stopping rule	Relative objective change $< 10^{-6}$ or 200 iterations	Convergence criterion
Normalization	Curtailment, ramp term, continuity term, fuel term normalized before weighting	Numerical conditioning and priority balancing
Battery power limit	± 0.40 MW	Prevents unrealistically large short-term buffering actions

Figure 1 shows the simulated renewable supply used in the study. It includes both surplus and shortage periods and is therefore sufficient to test storage behaviour and renewable curtailment within the assumed operational scenario.

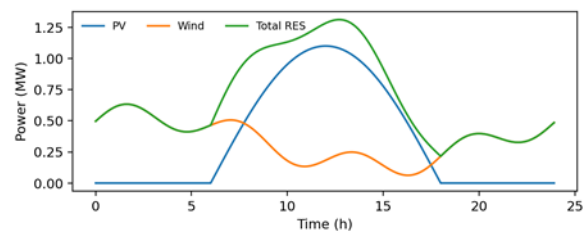


Fig. 1. Simulated 24 h renewable input for the reference case.

The profile contains both surplus and deficit periods and therefore provides an assumed, but stress-relevant test signal for battery buffering and curtailment behavior.

The mathematical formulation combines standard reduced-order models for battery state-of-charge evolution, electrolyzer hydrogen production, fuel-output aggregation, operational constraints, and ramp-rate limitation. These relationships are commonly used in energy-system and Power-to-X dispatch modelling. The paper does not claim novelty in the individual equations. Its methodological contribution is the integrated disturbance-aware supervisory formulation, including the combined objective function and the compact degradation-aware operating index used for comparative dispatch evaluation.

IV. SIMULATION SETUP AND DISTURBANCE SCENARIOS

The baseline case has no storage support and no dispatch optimization. It follows available renewable power subject to a minimum stable load and incurs cold-start penalties after reactivation. The optimized case adds battery buffering and deterministic smoothing with the ramp-rate limit. Two operating conditions are evaluated. The nominal case uses the synthetic renewable day without an imposed event. The stressed case introduces a one-hour renewable shortfall of 45% centered around noon. This event is not tied to a specific weather mechanism; rather, it serves as a clean disturbance-handling test. Such stress testing is appropriate for secure-systems-oriented evaluation because it isolates controller behavior under loss-of-supply conditions [1], [9].

The resilience score is defined as the ratio between mean electrolyzer power during the disturbance window and the pre-disturbance reference level. This keeps the resilience metric directly linked to process continuity. The main comparison is deliberately simple: a no-buffer baseline versus buffered optimized dispatch under the same renewable input. As a result, the reported percentage changes can be attributed to control and storage design rather than to a different resource profile.

The resilience score is adopted as the primary metric because it directly quantifies process continuity during the disturbance window and can be compared consistently across scenarios. It is intentionally narrow and is therefore complemented by uncertainty indicators, lower-tail production behaviour, and degradation trends. Additional resilience indicators that could be introduced in future work include minimum electrolyzer power during the disturbance, recovery time after disturbance, cumulative production loss, hydrogen-buffer depletion risk, and the number of operating-threshold violations.

V. RESULTS: SYSTEM STABILITY, RESILIENCE, AND DISTURBANCE HANDLING

Figure 2 compares electrolyzer dispatch during the stressed case. The baseline controller follows the renewable shortfall directly, whereas the optimized controller uses battery support and ramp shaping to maintain a flatter trajectory. This directly improves system stability because the power signal becomes less oscillatory. It also improves disturbance handling because the power level in the shortfall window is better preserved.

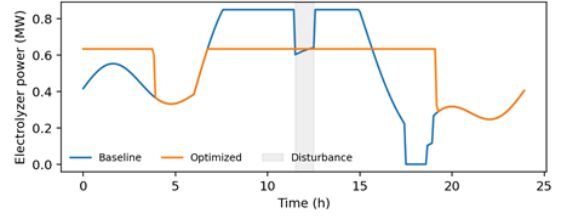


Fig. 2. Electrolyzer power during a forced one-hour renewable disturbance.

The optimized trajectory is flatter, which indicates better disturbance ride-through and lower dynamic stress.

The fuel effect follows the same pattern. Figure 3 shows cumulative daily fuel output. The optimized trajectory remains above the baseline because part of the renewable surplus is shifted through the battery instead of being wasted, and because the electrolyzer avoids repeated unstable operation around the minimum-load threshold. The reported fuel-output values should be interpreted as simulated control-oriented production indicators derived from an intentionally aggregated conversion model, not as plant-validated process-production estimates.

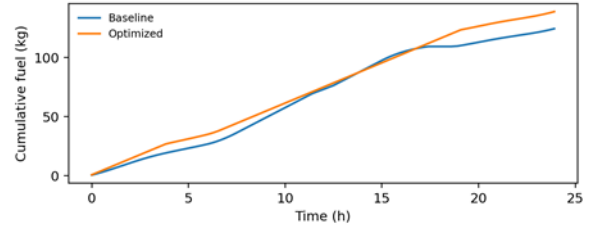


Fig. 3. Cumulative synthetic-fuel output in the stressed case.

The optimized trajectory remains above the baseline throughout the day, indicating improved fuel continuity.

The quantified results confirm the operational value of the proposed strategy within the reduced-order supervisory model. Under the stressed case, the optimized dispatch increases simulated daily fuel production by 11.6%, lowers electrolyzer-power variance by 66.3%, and improves the disturbance-window resilience score by 36.2%. These values should therefore be interpreted as model-derived indicators of dispatch quality under common assumptions, not as experimentally validated plant-scale production guarantees.

TABLE II. MAIN PERFORMANCE METRICS FOR THE STRESSED OPERATING CASE

Metric	Baseline	Optimized	Change
Daily fuel output (kg/day)	124.3	138.7	+11.6%
Electrolyzer power variance (-)	0.0646	0.0217	-66.3%
Resilience score (-)	0.734	1.000	+36.2%

VI. SENSITIVITY AND UNCERTAINTY ANALYSIS OF HYBRID OPERATION

Sensitivity analysis was added along two reviewer-critical axes: renewable-mix selection and storage sizing. The total installed renewable capacity was kept constant

while the PV/Wind ratio was varied, and battery capacity was swept from 0.0 MWh to 1.6 MWh. These two variables strongly influence curtailment, stability, and degradation accumulation.

TABLE III. SENSITIVITY ANALYSIS WITH RESPECT TO PV/WIND RATIO

PV/Wind ratio	Fuel output (kg/day)	Curtailment (MWh/day)	Degradation index (-)	Interpretation
70/30	96.1	5.05	7.10	Solar-heavy, noon peaking
50/50	134.9	1.82	4.28	Balanced mix
30/70	151.9	0.63	3.99	Wind-heavier, best resilience

The renewable-mix sweep shows that a PV-dominant design concentrates power around midday and therefore increases curtailment and dynamic stress. A more balanced or wind-heavier mix extends useful generation into non-daylight periods and reduces the burden on storage. In this study, the wind-heavier 30/70 PV/Wind split yields the highest fuel output, while the 50/50 case offers the most balanced engineering compromise. This trend is consistent with the literature on complementarity in hybrid renewable systems and storage-assisted dispatch [9], [13], [15].

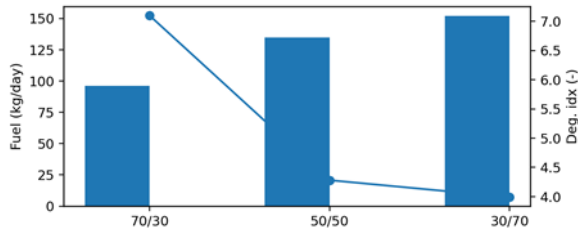


Fig. 4. Renewable-mix sensitivity results for constant total installed renewable capacity.

A more balanced or wind-heavier mix extends useful generation into non-daylight periods and reduces the burden on storage. In this study, the wind-heavier 30/70 PV/Wind split yields the highest simulated fuel output, while the 50/50 case offers the most balanced engineering compromise.

TABLE IV. SENSITIVITY ANALYSIS WITH RESPECT TO BATTERY ENERGY CAPACITY

Battery energy capacity (MWh)	Fuel output (kg/day)	Curtailment (MWh/day)	Degradation index (-)	Resilience score (-)
0.0	117.9	3.07	4.40	0.983
0.4	124.2	2.63	4.30	1.000
0.8	131.7	2.08	4.29	1.000
1.2	138.7	1.58	1.21	1.000
1.6	144.8	1.16	1.15	1.000

Moderate storage captures most of the modeled continuity benefit, while additional capacity above about 1.2 MWh yields diminishing returns.

To add uncertainty analysis, a Monte Carlo ensemble of 300 synthetic days was generated by perturbing hourly

photovoltaic and wind amplitudes. The photovoltaic perturbation used an 18% standard deviation and the wind perturbation a 12% standard deviation. These values are not intended as site-specific forecast-error statistics; they are deliberately chosen stress-test amplitudes that create substantial but plausible renewable variability around the deterministic profile. Hourly multipliers were sampled from truncated normal distributions, clipped to avoid negative generation, and linearly interpolated to the 5 min simulation grid. PV and wind perturbations were treated as independent in the present study, which is a simplifying assumption and a clear target for future work with measured site data and temporally correlated forecast errors. This uncertainty envelope tests controller robustness rather than providing a probabilistic production forecast [1], [9].

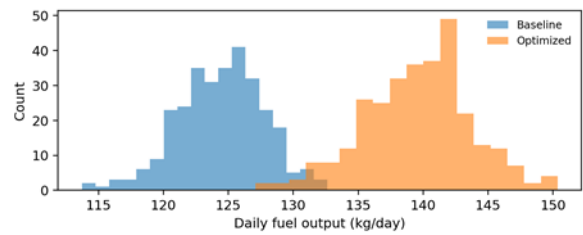


Fig. 5. Monte Carlo distribution of daily fuel output under renewable uncertainty.

The optimized distribution is shifted upward and narrower than the baseline distribution, indicating stronger robustness.

TABLE V. MONTE CARLO UNCERTAINTY SUMMARY FOR DAILY FUEL OUTPUT

Metric	Baseline	Optimized
Mean fuel output (kg/day)	124.5	139.6
5th percentile (kg/day)	119.0	132.4
Prob. fuel < 125 kg/day	0.54	0.00

The uncertainty results confirm that the optimized strategy remains preferable across a distribution of renewable days. It improves the ensemble mean and, more importantly, the lower-tail behavior: the 5th-percentile daily fuel output is substantially higher, and the probability of dropping below 125 kg/day is reduced to zero in the simulated ensemble. These Monte Carlo outputs remain model-derived operational indicators rather than experimentally validated plant-throughput measurements.

VII. DEGRADATION-AWARE OPERATION

Engineering realism is increased further by making degradation an explicit scheduling concern. A compact degradation-aware index is introduced for dispatch comparison:

$$D(t+1) = D(t) + \alpha |\Delta P_{EL}(t)| + \beta N_{SS}(t) + \gamma u_{over}(t) \quad (9)$$

where $D(t)$ denotes the accumulated degradation-aware operating index at time step t , $\Delta P_{EL}(t)$ is the electrolyzer

power change, $N_{ss}(t)$ is the start-stop event indicator or count, and $\gamma u_{over}(t)$ represents near-limit or over-operation. The coefficients α , β , and γ weight the contributions of ramp-induced stress, start-stop stress, and near-limit operating stress, respectively. The index is used as a comparative dispatch-level stress indicator rather than as a calibrated lifetime prediction model.

The first term penalizes ramp-induced stress, the second term penalizes start-stop events, and the third term penalizes sustained near-limit operation through

$$L_{high}(t) = \max \left[0, \frac{P_{EL}(t) - P_{high}}{P_{ELmax} - P_{high}} \right] \quad (10)$$

where $L_{high}(t)$ denotes the normalized high-load operation indicator at time step t , $P_{EL}(t)$ is the electrolyzer power, P_{high} is the threshold above which operation is treated as high-load operation, and P_{ELmax} is the maximum allowable electrolyzer power. The maximum operator ensures that the indicator remains zero below the high-load threshold and increases toward unity as the electrolyzer approaches its maximum operating power.

For the normalized comparisons reported here, $\alpha = \beta = \gamma = 1$ after scaling each term to the same order of magnitude. This makes the index transparent and reproducible while avoiding the false precision of uncalibrated aging constants.

The degradation index should therefore be read as a comparative operating-stress indicator rather than a lifetime predictor. In the present study, lower degradation-index values coincide with smoother optimized dispatch in both the sensitivity analysis and the main-case results. A natural next step is to calibrate the three coefficients against stack-specific aging data, especially for PEM systems exposed to frequent renewable cycling [5], [8].

Industrial and literature-reported experimental benchmarks are used in this study to check consistency of scale and dynamic behaviour, not to claim direct model validation. These benchmarks help assess whether the assumed supervisory operating ranges remain industrially plausible, but they do not provide one-to-one validation of the reduced-order model because the latter intentionally aggregates synthesis dynamics and does not reproduce plant-specific thermal and mass-balance behaviour.

In addition to the simulation-based evaluation, real industrial and experimental benchmarks help interpret the operating assumptions used in this paper. According to INERATEC's official ERA ONE information, the Frankfurt-Höchst plant is being scaled to 7 MW and up to 2,500 t/year of sustainable e-Fuels, while recycling up to 8,000 t/year of CO₂ [2], [3]. These values correspond to an average nominal fuel-production rate of approximately 285 kg/h, a specific fuel productivity of about 357 t/year per MW of installed plant capacity, and a CO₂-to-fuel ratio of about 3.2 t/t. The purpose of these benchmark values is not to claim one-to-one validation of the reduced-order supervisory model, but to anchor the study in a realistic industrial scale and to show that modular PtL plants already operate at non-trivial process-throughput levels.

TABLE VI. INDUSTRIAL-SCALE BENCHMARK DATA DERIVED FROM ERA ONE

Metric	Value	Meaning / source
Installed PtL capacity	7 MW	Official ERA ONE plant scale [2], [3]
Annual e-fuel output	2,500 t/year	Official ERA ONE production target [2], [3]
Annual CO ₂ recycle	8,000 t/year	Official ERA ONE CO ₂ recycle target [2]
Average nominal fuel output	≈285 kg/h	Derived from 2,500 t/year / 8,760 h
Specific fuel productivity	≈357 t/year/MW	Derived from 2,500 t/year / 7 MW
CO ₂ per tonne of fuel	≈3.2 t/t	Derived from 8,000 / 2,500

Published experimental results for industrial alkaline electrolysis provide more direct support for the dynamic constraints adopted in the model. Gu et al. investigated a 250-kW alkaline system and reported three characteristic response scales: current-step responses in the order of seconds, hydrogen-in-oxygen and pressure dynamics in the order of minutes, and thermal start-stop dynamics in the order of hours [7]. Their variable-load test included transitions from full load at 3,500 A and 1.7 MPa to minimum-load operation at 1,400 A and 1.7 MPa, as well as a lower operating point of 800 A and 0.6 MPa [7]. These results are directly relevant for secure operation because they show that even when electrical response is fast, gas-purity, temperature, and pressure variables impose slower and safety-relevant limits on plant dispatch.

TABLE VII. LITERATURE-REPORTED EXPERIMENTAL RESULTS RELEVANT TO CONTROL DESIGN

Metric	Value	Meaning / source
Industrial electrolyzer test platform	250 kW alkaline system	Representative for 100-kW to MW-class systems [7]
Cold start sequence	25 °C to full load at 90 °C	Temperature-limited start-stop transition [7]
Hot shutdown / hot start	75 °C shutdown, 70 °C restart	Thermal state matters for restart dynamics [7]
Variable-load test range	3,500 A at 1.7 MPa to 1,400 A at 1.7 MPa	Minimum-load transition without pressure change [7]
Extended low-load point	800 A at 0.6 MPa	Illustrates deeper turnaround with altered pressure [7]
Characteristic response scales	seconds / minutes / hours	Current / HTO-pressure / temperature dominated [7]
Review-based integration insight	Coupling factor >99%, practical STH efficiency around 10%	Battery support can improve operation but raises cost [6]

Taken together, these literature-reported experiments explain why a ramp-rate-limited, storage-buffered strategy is more credible than a pure renewable-following schedule.

In the present model, the battery absorbs fast renewable excursions so that the electrolyzer set-point remains within a slower operating envelope. This interpretation is consistent with the experimental hierarchy of time constants reported in [7] and with the review evidence that slower variables, such as temperature and pressure, become the limiting factors during variable operation [6].

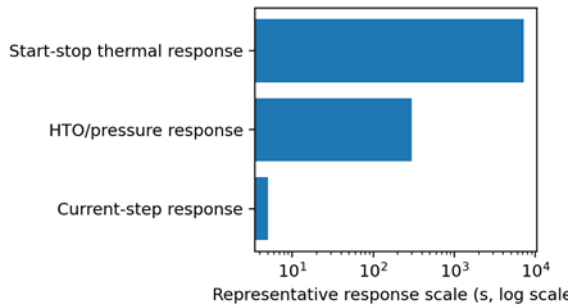


Fig. 6. Literature-reported response-scale hierarchy for industrial water electrolysis.

Fast electrical response coexists with slower gas-quality, pressure, and thermal transients, motivating ramp-limited supervisory control.

The benchmark data also sharpen the interpretation of the storage-sensitivity results. In the reference simulations, the main gain appears when battery capacity increases into the 0.8–1.2 MWh range. This should not be read as a universal plant-sizing result, but as an operational threshold above which the storage can meaningfully reshape sub-hour renewable disturbances before they propagate into minute-scale gas-quality and pressure constraints or hour-scale thermal penalties. Therefore, the reported improvement in resilience is supported both by the simulation results and by the dynamic limitations observed experimentally in industrial electrolysis systems [6]–[8].

VIII. DISCUSSION

The results demonstrate that the secure and resilient operation of a modular power-to-liquid plant depends on the coordinated behaviour of the hybrid PV-wind-storage supply system, not only on the nominal efficiency of the conversion chain. By combining deterministic supervisory optimization with battery buffering, disturbance-aware evaluation, sensitivity analysis, Monte Carlo uncertainty modelling, electrolyzer ramp constraints, and a degradation-aware operating index, the study shows that resilience, system stability, and disturbance handling can be materially improved through integrated system design.

A practical next step is hardware-in-the-loop validation. The control logic proposed in this paper is lightweight enough to be implemented in a MATLAB/Simulink supervisory layer or in an industrial PLC environment. A test bench that emulates renewable power, battery exchange, and electrolyzer constraints would make it possible to verify whether the simulated resilience gains remain visible when measurement delays, actuator saturation, and safety interlocks are introduced. Such a validation pathway would directly connect the

conference contribution to future secure-energy demonstrators.

A second limitation is that the degradation-aware index used here is intentionally compact. It is suitable for dispatch-level comparison because it captures the penalties associated with ramps, start-stop events, and near-limit operation, but it does not replace stack-specific aging coefficients obtained from long-duration laboratory campaigns. Future work should therefore combine supervisory scheduling with experimentally calibrated degradation parameters, especially for PEM systems exposed to frequent renewable cycling [5], [8].

The present work remains a reduced-order operational study rather than a full plant digital twin. The hydrogen-production block and the aggregate fuel-synthesis block are intentionally simplified for supervisory-control analysis. The reported trends are therefore most reliable for short disturbances and day-scale scheduling. For longer multi-hour shortages, seasonal renewable asymmetry, or forecast-based dispatch, the relative value of hydrogen buffering, day-ahead planning, and reserve management would likely increase. These effects should be explored in future work by coupling the present supervisory layer to longer-horizon forecasts and seasonally resolved renewable traces.

IX. LIMITATIONS AND FUTURE WORK

The present work remains a reduced-order operational study rather than a full plant digital twin. The hydrogen-production block and the aggregate fuel-synthesis block are intentionally simplified for supervisory-control analysis, and the hydrogen buffer is represented through continuity metrics rather than through an explicit mass-balance trajectory. Consequently, the reported trends are most reliable for short disturbances and day-scale scheduling, while longer shortages require explicit hydrogen-buffer dynamics, synthesis demand constraints, and buffer-depletion risk assessment.

A second limitation concerns uncertainty modelling. The Monte Carlo ensemble uses synthetic amplitude perturbations to test control robustness, but it does not reproduce site-specific solar irradiance, wind-speed correlation, seasonal asymmetry, forecast bias, or multi-day weather persistence. Future work should therefore replace the synthetic renewable traces with measured or reanalysis-based profiles and should evaluate day-ahead or model-predictive dispatch under forecast uncertainty.

A third limitation is the uncalibrated nature of the degradation index. The index is useful for comparing dispatch strategies because it penalizes ramps, restarts, and near-limit operation, but it should be validated against stack-specific aging measurements before being used for maintenance planning or lifetime prediction. A practical validation roadmap should include a 30–60 min renewable-drop ride-through test, start-stop cycling measurements, variable-load gas-quality and pressure monitoring, and battery-buffering tests that record state-of-charge swing, curtailed energy, and dispatched-power smoothness.

These limitations do not invalidate the control-oriented conclusions; rather, they define the boundary between a reduced-order supervisory study and the next stage of experimental and digital-twin validation.

X. CONCLUSION

The overall conclusion of this work is that modular e-fuel production under disturbed renewable input must be designed and operated as a coupled secure energy-conversion system. Within the adopted reduced-order supervisory formulation, the optimized strategy improves modelled fuel continuity, reduces electrolyzer-power variance, and enhances the disturbance-window resilience score relative to the no-buffer baseline. At the same time, the study shows that renewable-mix selection, battery sizing, and supervisory-control logic must be co-designed if secure and resilient operation is to be achieved under realistic renewable fluctuations. The main contribution is therefore methodological: a disturbance-aware, storage-buffered, degradation-conscious supervisory framework that is suitable for future extension toward higher-fidelity plant models and experimental validation.

ACKNOWLEDGMENT

This scientific report is funded by the Ministry of Education and Science in implementation of the Scientific Program „Security and Defence“, adopted by Decree No. 731 of 21.10.2021 and pursuant to Agreement No. D01-74/19.05.2022.

REFERENCES

- [1] A. Savachkin, W. Ardila-Rueda, D. Romero-Rodriguez, K. Hua, J.N.D.L. Cruz, Assessment and Optimization of System Resilience: A Critical Review. In: Borowik, G., Chmaj, G., Waszkowski, R. (eds) Models and Methods for Systems Engineering. Studies in Big Data, 2025, vol 165. Springer, Cham. https://doi.org/10.1007/978-3-031-76440-0_20.
- [2] INERATEC, “ERA ONE – e-Fuels made in Germany,” 2026. [Online]. Available: <https://www.ineratec.de/en/era-one-e-fuels-made-germany>. [Accessed April 17, 2026].
- [3] INERATEC, “INERATEC opens ERA ONE: Europe’s largest e-Fuel production plant goes into operation in Frankfurt,” Jun. 3, 2025. [Online]. Available: <https://www.ineratec.de/en/news/ineratec-opens-era-one-europes-largest-e-fuel-production-plant-goes-operation-frankfurt>. [Accessed April 17, 2026].
- [4] IEA (2025), *Global Hydrogen Review 2025*, IEA, Paris, [Online]. Available: <https://www.iea.org/reports/global-hydrogen-review-2025>, [Accessed April 17, 2026].
- [5] H. Sayed-Ahmed, A. I. Toldy, and A. Santasalo-Aarnio, “Dynamic operation of proton exchange membrane electrolyzers—Critical”, *Renewable and Sustainable Energy Reviews*, Volume 189, Part A, 2024, 113883, ISSN 1364-0321, <https://doi.org/10.1016/j.rser.2023.113883>.
- [6] V. A. Martinez Lopez, H. Ziar, J. W. Haverkort, M. Zeman, and O. Isabella, “Dynamic operation of water electrolyzers: A review for applications in photovoltaic systems integration”, *Renewable and Sustainable Energy Reviews*, 2023, ISSN 1364-0321, <https://doi.org/10.1016/j.rser.2023.113407>.
- [7] J. Gu et al., “Experimental studies on dynamic performance of 250-kW alkaline electrolytic system”, *Journal of Power Sources*, Volume 592, 2024, 233920, ISSN 0378-7753, <https://doi.org/10.1016/j.jpowsour.2023.233920>.
- [8] H. Y. Jung, Y. S. Jun, K.-Y. Lee, H. S. Park, S. K. Cho, and J. H. Jang, “Effect of Ramping Rate on the Durability of Proton Exchange Membrane Water Electrolysis During Dynamic Operation Using Triangular Voltage Cycling”, *Journal of Electrochemical Science and Technology*, vol. 15, no. 2. The Korean Electrochemical Society - English Journal, pp. 253–260, 31-May-2024.
- [9] Giedraityte A, Rimkevicius S, Marciukaitis M, Radziukynas V, Bakas R. Hybrid Renewable Energy Systems—A Review of Optimization Approaches and Future Challenges. *Applied Sciences*. 2025; 15(4):1744. <https://doi.org/10.3390/app15041744>.
- [10] Schmidt, P., Batteiger, V., Roth, A., Weindorf, W. and Raksha, T. (2018), Power-to-Liquids as Renewable Fuel Option for Aviation: A Review. *Chemie Ingenieur Technik*, 90: 127-140. <https://doi.org/10.1002/cite.201700129>
- [11] C. Huang et al., “The complementary role of E-fuel in decarbonizing transportation and stabilizing the power grid”, *Renewable and Sustainable Energy Reviews*, Volume 224, 2025, 116033, ISSN 1364-0321, <https://doi.org/10.1016/j.rser.2025.116033>.
- [12] V. Dieterich, A. Buttler, A. Hanel, H. Spliethoff and S. Fendt. “Power-to-liquid via synthesis of methanol, DME or Fischer–Tropsch-fuels: a review.”, *Energy & Environmental Science*, 2020, 13, 3207-3252, <https://doi.org/10.1039/D0EE01187H>.
- [13] A. A. Kebede, T. Kalogiannis, J. Van Mierlo, M. Bercibar, “A comprehensive review of stationary energy storage devices for large scale renewable energy sources grid integration”, *Renewable and Sustainable Energy Reviews*, Volume 159, 2022, 112213, ISSN 1364-0321, <https://doi.org/10.1016/j.rser.2022.112213>.
- [14] P. Gabrielli, M. Gazzani, E. Martelli, and M. Mazzotti, “Optimal design of multi-energy systems with seasonal storage”, *Applied Energy*, Volume 219, 2018, Pages 408-424, ISSN 0306-2619, <https://doi.org/10.1016/j.apenergy.2017.07.142>.
- [15] Schmiegel, Armin U., *Energy Storage Systems: System Design and Storage Technologies* (Oxford, 2023; online edn, Oxford Academic, 22 June 2023), <https://doi.org/10.1093/oso/9780192858009.001.0001>, [Accessed 17 April, 2026].

Analysis of Models for Estimating Electricity Losses in Distribution Networks

Misho Matsankov

Center of competence "Smart mechatronic, eco and energy saving systems and technologies";
Faculty of Electronics and Automation,
Plovdiv branch
Technical University of Sofia
Sofia, Bulgaria
mishel@tu-plovdiv.bg

Abstract—The design of renewable energy sources and their connection to the electrical grids at different voltage levels leads to changes in the mode parameters of the grid. Electrical energy losses are of both technical and economic interest. The report examines the most commonly used models for estimating electricity losses in low-voltage distribution networks, depending on the available data under operational conditions. It is proposed to use an improved model with increased accuracy, in the application of which the seasonality coefficient is taken into account.

Keywords— Electricity losses, electrical networks, low voltage, models.

I. INTRODUCTION

In recent years, the attention paid to ecology has been increasing. Environmental requirements for exhaust gases are increasing, which requires optimization of combustion plants and processes [1, 2]. All of these contribute to the development of renewable sources of electrical energy. The large-capacity renewable sources designed and connected so far were mostly connected to medium and high voltage networks, depending on the specific situation and the network configuration. This led to the depletion of the capacity of some of the power lines. This made low-voltage networks particularly attractive. As a result, increasing number of small-scale solar power plants and zero-consumption buildings are joining into low voltage network [3, 4]. Their production depends not only on meteorological conditions, but also on some other features, such as the cleanliness of their surface [5]. Therefore, monitoring the parameters of the power plants allows optimizing their production [6]. As a result, low-voltage networks undergo rapid operational changes [8-9]. The motivation that owners receive is a combination of the affordable price of the systems, a simplified procedure for obtaining a design and construction permit [10-12]. The creation of energy independence is also not in last place.

Despite their local impact, all of them taken together have a significant impact on the operating parameters of the electrical networks. Power losses and, respectively, electrical energy are among the main mode parameters that will be affected. They play a crucial role in the overall efficiency of the electricity grid, affecting operating costs, reliability and resilience of the grid, which is why the accuracy of the models for their assessment is of utmost importance. That is why they represent a constant operational and economic interest. Their share is significant in low-voltage networks, where the currents are high and in some cases the power lines are quite long. Accurate quantification of annual technical energy losses in low-voltage distribution networks is important for grid planning, investment in loss reduction and performance benchmarking. However, an assessment based on high-resolution energy flow time series (e.g., 8760-hour simulation with node/branch level load profiles) is often not possible in practice due to limited metering, uncertain customer load distribution and incomplete feeder data. This has motivated long-term work on methods for estimating annual losses that compress the temporal variability of the load into one or more scalar descriptors (e.g., equivalent loss duration/maximum loss time, load schedule shape descriptors) and/or the spatial complexity of the network into reduced representations with equivalent network diagrams [13, 14]. Large-scale analysis of data from distribution network operators highlights both the significance and heterogeneity of losses in low-voltage networks, with their share in peak load conditions varying across service areas and depending on the network configuration [15]. A large part of the research on the impact of photovoltaic installations on low-voltage networks is that photovoltaic installations can reduce or increase technical losses, depending on the level of penetration, the coincidence with local consumption (self-consumption) and the phase distribution. Detailed studies

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.150>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

of the networks report non-monotonic loss behavior, including regimes where losses decrease as photovoltaic installations compensate for local load, and regimes where reverse power flow and voltage increases become significant and can increase losses and operational risks [7-9, 16]. The sensitivity of losses to the location of photovoltaic installations and their penetration depth is reflected in [17]. Analysis methods have begun to address the limitations of observability by reconstructing unmetered consumption and estimating time-varying losses from smart meter data using learned typical load profiles and probabilistic inference [18]. A large number of authors working on low-voltage networks and photovoltaic systems still consider losses primarily as a result of simulation, rather than as a quantity governed by explicitly specified simplified evaluation functions whose parameters (e.g. “equivalent length”, profile-based loss factors, or time scaling) can be calibrated and transferred between supply lines and photovoltaic system deployment scenarios [7, 8, 19, 20]. There is a clear opportunity to more systematically couple the transformation of net load supplied by photovoltaic systems—including self-consumption, power reverse flow periods, and phase distribution—with simplified loss estimation models that remain interpretable, calibratable, and easy to compute, while maintaining fidelity to the mechanisms highlighted by detailed studies of power lines (voltage limitations, unbalance, and power reversal) [7, 8, 16, 21].

Deterministic families of methods such as those based on maximum loss time (equivalent loss duration), “2t” approximations, graphical integration, and average/RMS node loads—have been comparatively reviewed for low voltage industrial or workshop-type networks, with explicit discussion of required input data and typical error sources (e.g., inaccurate estimation of the time of largest losses, ignoring load-shape effects, neglecting conductor heating and contact resistances) [23-25].

A particularly active deterministic thread focuses on the equivalent-duration (maximum-loss time) concept, where annual loss energy is approximated as peak (or reference) loss power multiplied by an “equivalent” number of hours at that level. Recent analysis emphasizes that the empirical relationships used to estimate this duration can exhibit limited validity under strongly uneven or seasonal load schedules, motivating tighter applicability ranges and potentially new empirical models for modern operating conditions [22]. Complementary to these temporal compressions, low voltage -specific work on equivalent resistance in short, equipment-dense shop/industrial networks highlights that non-cable components (e.g., switching-device contact resistances) and temperature-dependent conductor resistance can materially affect loss estimates, and therefore should be included when constructing reduced network equivalents intended for practical calculations [24].

In parallel, a statistically grounded line of research treats loads (and thus currents) as random variables and computes expected $I^2 R$ losses from second-moment information (e.g., mean and variance), rather than explicit time-series simulation. Shenkman’s early formulation of statistical techniques for energy-loss computation provides

foundational probabilistic machinery for estimating losses from load statistics [27]. This approach was subsequently specialized toward low voltage distribution networks using variance-based loss computation, directly to capture the quadratic dependence of losses on loading without full temporal detail [26]. Planning-oriented extensions further demonstrate how variance-based estimators can support distribution-network studies when only partial data are available [30].

Between these deterministic and probabilistic poles, several “simplified” or hybrid feeder-level models combine feeder characteristics (e.g., length, peak demand) with load profile descriptors (e.g., load factor or statistical moments of daily load curves), aiming to operate across different regimes of data availability [28, 29]. Collectively, this literature suggests a spectrum of annual-loss estimation methodologies with distinct assumptions about load synchrony, spatial load distribution stability, and the availability/quality of schedule statistics. At the same time, the retrieved works do not appear to provide a single, unified head-to-head comparison of all classical approximation families on common low voltage feeders, implying that integrated benchmarking against detailed load-flow remains an open and practically relevant research task [22-25, 28-30].

The most commonly used methods for estimating electrical energy losses in low-voltage distribution networks are examined, depending on the information provided. It is proposed to take into account the seasonality coefficient, which would increase the accuracy of the models. Depending on the operating conditions, the network configuration and its declared voltage, different methods are applied to calculate the network operating parameters, such as voltage levels in the nodes, power losses and electrical energy.

II. MATERIALS AND METHODS

The study examines a branch of a low-voltage electrical network from a small settlement with large section lengths and low density of electrical loads. The diagram in Fig. 1 shows the section lengths and powers in maximum load mode without taking into account the impact of installed renewable sources.

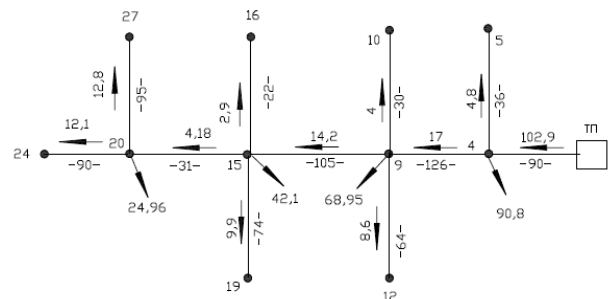


Fig. 1. electrical diagram of a low voltage distribution network

All consumers have installed photovoltaic systems that meet the latest requirements described in [10] and [11].

Methods for calculating the modes of electrical networks, voltage levels in nodes, power and energy losses

are applied depending on the declared voltage, network configuration and operating conditions [31-33]. Models for calculating technical losses of electricity in low-voltage electrical networks require different available information. The most commonly used models for determining electricity losses in low voltage electrical networks are presented below:

A. Model with the equivalent length of the power line and the filling factor k , of the load profile

Electricity losses in low-voltage electrical networks based on operational data are determined by the (1) from [21, 24]:

$$\Delta W = k_H \frac{W^2 \cdot (1 + \operatorname{tg}^2 \varphi) \cdot L_e}{s \cdot T} \cdot \frac{1 + 2 \cdot k_3}{3 \cdot k_3} \quad (1)$$

Where:

W is the electricity delivered to consumers for a specified period;

T is consumption period (expressed in days);

s is the cross-section of the conductor in the main line;

L_e is the length of the power line;

$\operatorname{tg} \varphi$ is the reactive power factor;

K_n - the coefficient taking into account the nature of the distribution of loads along the length of the power line and the inequality of the loads of the phases.

The equivalent length of the line is determined by (2).

$$L_e = L_M + k_{2-3} \cdot L_{2-3} + k_1 \cdot L_1 \quad (2)$$

Where:

L_M is the length of the highway;

L_{2-3} is the length of two-phase and three-phase deviations and the corresponding coefficient is $K_{2-3} = 0,44$;

L_1 is the length of single-phase deviations and the corresponding coefficient is $K_1 = 0,22$;

The coefficient K_n is determined by (3).

$$k_H = 9,67 - 3,32d_p - 1,84d_p^2 \quad (3)$$

Where d_p is that part of the energy that is used in the domestic sector

When using (1) to determine the losses in N lines with a total length of the mains $L_{M\text{sum}}$, two-phase and three-phase deviations $L_{2-3\text{sum}}$ and single-phase deviations $L_{1\text{sum}}$, the average released electricity in one line $W = W_s / N$ is taken, where W_{sum} is the total released energy in N lines. The coefficient K_n , determined by (3), is multiplied by the coefficient K_n , which takes into account the inequality of the lengths of the lines and the current densities in the mains.

$$k_N = 1,25 - 0,14d_p \quad (4)$$

When there is no data on the load schedule filling factor and the reactive power coefficient, $k_3 = 0,3$; $\operatorname{tg} \varphi = 0,6$ is assumed.

B. Model using the total length L_{sum} and the fictitious duration t of power losses

$$\Delta W = \Delta P_c \cdot L_{\Sigma} \cdot \tau \quad (5)$$

Where ΔP is the average value of power losses per 1 km of the power line at maximum load.

$$\Delta P_c = 3 \cdot \left(\frac{S_H \cdot k_{HT}}{\sqrt{3} \cdot U} \cdot k_p \right)^2 \cdot r \quad (6)$$

Where:

S_n is the nominal power of the power transformer;

K_{nt} is the average load of the transformer at maximum load;

K_p is the load distribution coefficient along the length of the line;

d is the active resistance per 1 km of the conductor.

C. Model with determination of voltage losses to the electrically farthest node from the transformer substation

This approach allows to determine the power losses through the voltage losses to the electrically most remote node from the transformer station, taking into account the unevenness of the load of the phases in the low-voltage network. The results of the measurements of the voltage levels in the transformer station and at the electrically most remote point of the network, the phase currents I_A, I_B, I_C of the main line during the maximum load are used as the initial information.

$$\Delta W_{\%} = K_{mn} \cdot K_{al} \cdot \Delta U_{cr\%} \cdot \tau \quad (7)$$

Where:

$U_{av\%}$ is the average value of voltage losses.

K_{al} is the coefficient of additional losses, which takes into account the unevenness of the phase load.

$$k_{al} = 3 \cdot \frac{I_A^2 + I_B^2 + I_C^2}{(I_A + I_B + I_C)^2} \cdot \left(1 + 1,5 \frac{R_H}{R_{\phi}} \right) - 1,5 \cdot \frac{R_H}{R_{\phi}} \quad (8)$$

Where:

R_H and R_{ϕ} are the resistances of the neutral and phase conductors.

K_{to} - the coefficient which depends on the network configuration and load density.

$$K_{mn} = \frac{K_b \cdot 2r}{(2r \cdot \cos^2 \varphi + x \cdot \sin 2\varphi)} \quad (9)$$

Where:

r and x are the active and reactive resistance of the highway;

K_b - the branching coefficient of the circuit [31, 34].

D. A probabilistic approach with a known maximum load P_{max} and a specified type of load schedule.

The coefficient k_p is determined depending on the available data [31, 34].:

the mathematical expectation of the maximum load P_T according to the typical load schedule is determined by (10):

$$k_p = \frac{\sqrt{\left(\frac{\beta V \cdot \overline{P_T}}{200}\right)^2 + \overline{P_T} \cdot P_{max}} - \frac{\beta V \cdot \overline{P_T}}{200}}{\overline{P_T}} \quad (10)$$

Where:

β - the confidence coefficient ($\beta_B = 2$ at a confidence probability of 0.975);

B_p - the coefficient of variation of the maximum load.

When the value of the mathematical expectation of the maximum active power P_{max} is known:

$$k_p = \sqrt{\frac{\overline{P_{max}}}{\overline{P_T}}} \quad (11)$$

When the amount of electricity consumed W per year is known:

$$k_p = \sqrt{\frac{W}{W_T}} \quad (12)$$

The annual electricity consumption W corresponding to the given load schedule is determined by (13).

$$W_T = \frac{\sum_{k=1}^{12} m_k \cdot \overline{P_{CT}} \cdot \sum_{j=1}^{12} k_{pj} \cdot \sum_{i=1}^{24} P_{ik}}{1200} \quad (13)$$

where k_{pj} is the seasonality coefficient;

Ric is the mathematical expectation of the active power in the i_{th} hour of the k_{th} season, where t is the number of days in the month.

III. RESULTS AND DISCUSSION

The results of the calculations performed using the compiled algorithms of the four models are summarized in Fig. 2. The errors made in determining electricity losses

depending on the load schedule fill factor when applying the following models are shown:

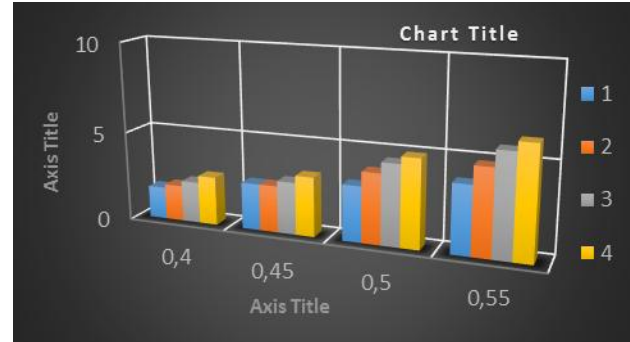


Fig. 2. distribution of errors in determining losses depending on the load schedule fill factor

1 - using the equivalent length of the power line and the load schedule filling factor;

2 - with the total length of the power lines and the fictitious duration:

3 - with determination of the voltage losses to the electrically farthest node from the transformer station;

4 - with a probabilistic approach with a known maximum load P_{max} and a given typical load schedule.

The error is calculated relative to the basic method for approximation discretization of the known load schedule with a step shape at a very high degree of discretization.

Fig. 2. Errors in determining electricity losses depending on the load schedule fill factor when applying models 1+4 for a low voltage distribution network. It is established that the error is the largest when applying the second model, and the smallest when applying the fourth model.

As the load schedule fill factor increases, the allowable calculation error increases.

IV. CONCLUSIONS

- The model using the equivalent length of the power line and the load schedule fill factor is recommended in the absence of measurements and the availability of data on energy consumption in the residential sector.
- The most inaccurate model is the one using the total length L_{sum} and the fictitious duration τ due to its approximate selection.
- A model with determination of voltage losses to the electrically most remote node from the substation, using control measurements of voltages in the supply node and phase currents in the highway during maximum load, is more accurate than the first model. The approach is relatively easy to implement, but it is difficult to determine the coefficient K_{mp} .
- The first three models can be considered as evaluative in the case of an insufficiently developed information system for calculating modes and losses in low voltage networks.
- The fourth model is the most accurate and promising. It can be used without problems in modern technical

equipment and the coordination of the work of distribution networks and regional dispatching services.

V. ACKNOWLEDGMENTS

The authors would like to express their gratitude to the management of the project No. BG16RFPR002-1.014-0005 Competence Center "Intelligent Mechatronics, Eco- and Energy-Saving Systems and Technologies" for their financial support.

REFERENCES

- [1] A. N. Sapargaliyeva, A. M. Dostiyarov, D. Umyshev, A. K. Baidalina, A. S. Begimbetova, N. N. Sarakeshova and Z. F. Ozhikenova, "Experimental Investigation of an Air-Staged Swirl Burner with Hemispherical Stabilizer for Low-NO_x Combustion", MDPI February 2026 19 (4), DOI:10.3390/en19040897.
- [2] A. M. Dostiyarov, A. N. Sapargaliyeva, A. K. Yamanbekova and I. K. Iliev, "Development of a new front heat generator device and results of numerical simulation on Comsol Multiphysics", 9th International Conference on Energy Efficiency and Agricultural Engineering 2024, DOI:10.1109/EEAE60309.2024.10600586.
- [3] K. Seymenliyski, A. Yovkov, E. Zaerov, V. Todorov, R. Simionov and H. Mihaylov, "Modern Technological Solutions for Passive Buildings and Buildings with Zero Energy Consumption", Telecommunications and Remote Sensing juli 2025 (pp.87-99), DOI:10.1007/978-3-031-99332-9.
- [4] N. Mihaylov, B. Evstatiev, S. Kadirova, T. Gueorguiev, T. Georgieva and A. Evtimov, "Load Profile of Typical Residential Buildings in Bulgaria", IOP Conference Series: Earth and Environmental Science 2018, DOI: 10.1088/1755-1315/172/1/012035.
- [5] M. Vassilev, B. Stankov, P. Zlateva, and M. Karimoldanova, "Influence of Thermophoresis on the Deposition of Limestone Dust Particles on Solar Panel Surfaces"
- [6] A. Chekichev, A. Parushev, R. Popov, N. Paunkov, M. Bundeve, Microprocessor System for Studying the Operating Characteristics of the Photovoltaic Panels, TELECOM 2024, DOI: 10.1109/TELECOM63374.2024.10812301
- [7] G. Fernández, N. Galan, D. Marquina, D. Martínez, A. Sanchez, P. López, H. Bludszuweit and J. Rueda. "Photovoltaic Generation Impact Analysis in Low Voltage Distribution Grids", Energies 2020, 13(17), DOI: 10.3390/en13174347
- [8] J. Bendík, M. Cenky, B. Cintula, A. Belán, Ž. Eleschová and P. Janiga. "Stochastic Approach for Increasing the PV Hosting Capacity of a Low-Voltage Distribution Network". DOI: 10.3390/pr11010009.
- [9] Y. Gabdullin and B. Azzopardi, "Impacts of Photovoltaics in Low-Voltage Distribution Networks", Energies 2022, 15(18), 6731; DOI:10.3390/en15186731.
- [10] Law on Territorial Planning, Last amended 17 Oct 2025.
- [11] Renewable Energy Sources Act. Last amended on Nov 14, 2025.
- [12] Standard BDS EN 50160, Last amended 2023.
- [13] E. Yu. Gracheva, Z. M. Shakurova and R. E. Abdullazyanov, "A comparative analysis of the most common deterministic methods for the calculation of electricity losses in industrial networks", Power engineering: research, equipment, technology, 2019, 21(5):87-96, DOI:10.30724//1998-9903-2019-21-5-87-96.
- [14] E. Gracheva and A. Alimova, "Calculation Methods and Comparative Analysis of Losses of Active and Electric Energy in Low Voltage Devices", International Ural Conference on Electrical Power Engineering 2019, DOI:10.1109/URALCON.2019.8877627
- [15] M. Kornatka and A. Gawlak. "An Analysis of the Operation of Distribution Networks Using Kernel Density Estimators", Energies 2021, 14(21), 6984; DOI:10.3390/en14216984.
- [16] I. C. Torres, G. F. Negreiros and C. Tiba. "Theoretical and Experimental Study to Determine Voltage Violation, Reverse Electric Current and Losses in Prosumers Connected to Low-Voltage Power Grid". Energies 2019, 12 (23), 4568; DOI:10.3390/en12234568.
- [17] A. Gawlak and M. Kornatka, "Analysis of the Impact of Photovoltaic Generation on the Level of Energy Losses in a Low-Voltage Network". Energies 2024, 17 (23), 5957, DOI:10.3390/en17235957.
- [18] R. Telford, R., B. Stephen, J. Browell and S. Haben. "Dirichlet Sampled Capacity and Loss Estimation for LV Distribution Networks With Partial Observability", IEEE Transactions on Power Delivery, DOI:10.1109/TPWRD.2020.3025125
- [19] M. T. Au and C. H. Tan. "Energy flow models for the estimation of technical losses in distribution network". IOP Conference Series: Earth and Environmental Science 16(1):2035, DOI:10.1088/1755-1315/16/1/012035
- [20] M. Verdelho, R. Prata, P. Carvalho and J. Machado. "Impact of PV distributed generation on EDP distribuição LV grid losses". CIRED - Open Access Proceedings Journal 2017 (1):2342-2345, DOI:10.1049/oap-cired.2017.0306.
- [21] O. Ivanov, B. Neagu, A. Cibotărică and M. Gavrilăş. "Multiobjective Prosumer Surplus Management for Optimal Microgrid Operation". 10th International Conference on ENERGY and ENVIRONMENT 2021.
- [22] V. Bodunov, G. Oleksandr, T. Kulko and A. Prystupa, "Estimation of Existing Models of the Maximum Duration of Active Energy Losses in Distribution Networks", Bulletin of the National Technical University «KhPI» Series: New solutions in modern technologies, 2023, DOI:10.20998/2413-4295.2023.02.01
- [23] E. Gracheva, Z. Shakurova and R. Abdullazyanov, "A comparative analysis of the most common deterministic methods for the calculation of electricity losses in industrial networks " Power engineering: research, equipment, technology, 2019 21(5):87-96. DOI:10.30724//1998-9903-2019-21-5-87-96
- [24] E. Gracheva and A. Alimova, "Calculation Methods and Comparative Analysis of Losses of Active and Electric Energy in Low Voltage Devices", 2019 International Ural Conference on Electrical Power Engineering (UralCon), 2019.
- [25] E. Gracheva, A. Alimova, "Сравнительный анализ и исследование методов расчета потерь электроэнергии в системах электроснабжения промышленных предприятий", 2018.
- [26] O. M. Mikic, "Variance-Based Energy Loss Computation in Low Voltage Distribution Networks", IEEE Transactions on Power Systems, 2007
- [27] A. Shenkman, "Energy loss computation by using statistical techniques", IEEE Transactions on Power Delivery, 1990
- [28] M. T. Au and C. H. Tan, "Energy flow models for the estimation of technical losses in distribution network", IOP Conference Series: Earth and Environmental Science, 2013
- [29] T. M. Anthony, M. Yusoff, "A simplified approach in estimating technical losses in distribution network based on load profile and feeder characteristics", 2008 IEEE 2nd International Power and Energy Conference, 2008
- [30] J. Dickert, M. Hable and P. Schegner, "Energy loss estimation in distribution networks for planning purposes", 2009 IEEE Bucharest PowerTech, 2009, DOI:10.1109/PTC.2009.5281997
- [31] P. Notov and St., Nedeltcheva, Electroenergetics, Volume 1, TU – Sofia Publishing house, Sofia, 2009.
- [32] P. Notov and St., Nedeltcheva, Electroenergetics, Volume 2, TU – Sofia Publishing house, Sofia, 2009.
- [33] St. Nedeltcheva, Electrical networks and systems with decentralized generating sources, ISBN 978-619-167-348-3, TU – Sofia Publishing house, Sofia, April 2018.
- [34] Nedelcheva S., Application of mathematical models for determining the losses of electricity in CH and HV power lines. Anniversary scientific conference, Sliven'97.

Negative Impact of Renewable Energy: Critical Analysis

Ventsislava Nikolova-Minkova

Department of Social and Economic Sciences
Technical University of Gabrovo
Gabrovo, Bulgaria
minkova.ventsislava@gmail.com

Abstract—The importance of renewable energy has grown enormously in recent years, with the EU's target for renewables to achieve a share of 42.5% of gross energy consumption by 2030. This is related not only to stimulating technological developments in the field and increasing investments, but also to legislative changes to accelerate the modernization of networks, remove regulatory barriers, regulate the activities of prosumers, and encourage consumers and producers to increase consumption. In this study, we aim not only to define the essence of renewable energy sources, but also to prepare a critical analysis of the scientific literature addressing the issues of the negative impact of renewable sources on the environment. In this regard, by applying a bibliometric analysis of the existing literature in Scopus, we highlight the leading specialists in the field and their citation, which is an expression of the significance of the published scientific ideas. Through keywords co-occurrence analysis, we reveal the leading topics around which specialists' research is focused. As a result, we present and summarize the main negative effects of renewable energy sources. In conclusion, and based on the analysis, we confirm our hypothesis that the environmental risks of renewable energy sources are insufficiently analysed and contradict the assumptions of the concept of sustainable development.

Keywords— *bibliometric analysis, negative impact, renewable energies.*

I. INTRODUCTION

In the scientific and specialized literature, the term “renewable energy” occurs as early as the beginning of the 20th century, when it is used as a contrast to exhaustible energy sources [1] - [3]. Of course, the meaning given at the beginning of the century differs significantly from the meaning that the term acquired during the period of World War II or during the energy debates of the 1970s [3]. In modern times, the concept of renewable energy has become a leading policy around the world and occupies a central role in the fight against climate change. Its defining

features, mechanisms for creation and application, as well as its impact on the environment and society in the long term are critical in determining effectiveness and sustainability in the context of the concept of sustainable development.

The relevance of the topic we are considering stems from the EU's goals to expand the share of renewable energy sources (RES) in the overall energy mix. By targeting 42.5% renewable energy consumption by 2030, the EU is pushing Member States to increase investment in this area and increase renewable energy production areas. This will reduce energy dependence on fossil fuels on the one hand, and on the other hand, it will also limit dependence on the main producers and exporters of these fuels. This is directly related not only to the specifics of renewables, but also to the widely accepted statement that they are a better substitute for fossil fuels for several main reasons: (1) limit environmental pollution compared to fossil fuels; (2) limit the extraction of conventional natural resources; (3) have a positive impact on the socio-economic status of people.

Analysing the specialized literature, we reveal the wide range of areas of analysis in the field of renewable energy. The definitive features and sources of renewable energy are discussed and described in detail by [4] - [8]. Several studies [9] - [12] raise the question of the role of renewable energy sources in achieving the goals of the concept of sustainable development. Many studies are also devoted to the policies and practices of introducing renewables at local level [13] - [15], the economic and social effect they cause [16]-[17] or the benefits of their introduction in specific productive sectors [18]. A significant place is also occupied by research focusing on the impact of renewable energy sources [19]-[25].

However, the scope of studies on the negative impact of renewables in the long term remains limited, which for us represents a significant research gap.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.66>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

Therefore, in this study, we aim not only to define the essence of renewable energy sources, but also to prepare a critical analysis of the limited scientific literature concerning the negative impact of renewable sources on the environment. Thus, we choose renewable energy as the object of research, and the subject of our study is the negative impact that renewable energy sources have on the environment and society in the long term.

The hypothesis, which we will seek to prove in the course of our work, is that: The negative impact of renewables on the environment and society in the long term is insufficiently analysed.

In the next part of the development, we present some of the definitive features of renewable energy. The empirical part of this work includes conducting a bibliometric and keyword co-occurrence analysis of specialized literature from the Scopus database. As a result, we reveal and summarize the main negative effects of renewables. In conclusion, and based on the analysis, we confirm our hypothesis that the environmental risks of renewable energy sources are insufficiently analysed and contradict the formulations of the concept of sustainable development.

II. MATERIALS AND METHODS

A. Literature Review

Without examining in depth the definitive features of renewable energy and its sources, we can generally present it as „... *energy obtained from naturally repetitive and persistent flows of energy occurring in the local environment.*“ [4, p.3] while „*Non-renewable energy is energy obtained from static stores of energy that remain underground unless released by human interaction*“ [4, p.3].

According to [24], renewable energy sources, which are often defined by the scientific community as “clean” energy sources, are powered by naturally renewable energy sources in nature and can be used independently of each other.

For [15], renewable energy goes beyond the framework of innovative technical alternatives to fossil fuels and symbolises the expansion of societal values through the transformation towards sustainable and nature-friendly energy production and consumption.

Considering the above and the broad interpretation of the definitive features of renewable energy in specialized literature, energy transition strategies, and regulatory documents, for the purposes of our research we perceive renewable energy as *energy generated by naturally occurring processes in nature and assimilated through innovative technological solutions.*

Specific renewable energy sources (see Fig. 1) encompass the technologies and facilities through which natural energy flows are transformed into electricity, such as solar energy, wind energy, hydropower, geothermal energy, and biomass energy [26].

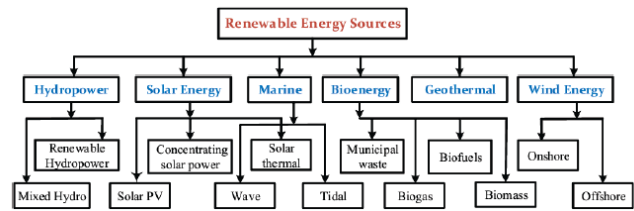


Fig. 1. A summary of the most common renewable energy sources [27].

Renewable technologies (see Fig. 1) are also those whose long-term impact on the environment needs to be analysed to establish their sustainability. Therefore, in the following lines we set ourselves the task of briefly clarifying their essence.

Hydropower is generated using the mechanical energy of flowing water (rivers and streams) and capturing it through pipelines driving generators to create electrical energy [24].

Marine/ocean energy – a type of hydropower, in terms of the natural resource used to create energy, but here it is generated by the tides and by the waves of the marine/ocean. This type of energy is new and still insufficiently developed and used due to the need for large investments for the development of technology [24].

Solar energy can be produced through systems of several types and functions, such as photovoltaic cells which converting direct sunlight into electrical energy, thermal solar systems, or systems heating liquids through sunlight to produce steam to drive a turbine that produces electricity [5], [24].

Bioenergy is produced from several types of residues from biological sources (forestry residues, animal residues, industrial residues, crops, sewage waste, or municipal solid waste) [8]. The production of energy from biological resources, when they are residue or waste, does not compete with other land resources (as is the case with the production of bioenergy from crops plantations that displace other crops and threaten biodiversity) [24].

Geothermal energy is produced by recovering hot water or steam rising to the surface of the earth from the Earth’s naturally occurring geothermal processes. Once it reaches the surface, the steam/hot water is used to drive a steam turbine that produces electricity. A key point in the utilization of geothermal energy is that the location where geothermal plants can be opened is severely limited, due to the specific requirements of the natural environment in which geothermal energy is stored [28].

Wind energy is produced by a wind turbine, which converts the kinetic energy of the wind into mechanical energy [5]. Subsequently, mechanical energy is converted again (through a generator) into electrical energy [28]. According to [9], wind energy generation is one of the most economical renewable energy systems.

In this literature review, we have briefly presented the specifics of energy sources, and in the next part we will focus on the overall negative effect they cause. Although in scientific literature the negative side of renewable energy

sources remains in the background, the issue has gained greater significance in the last 3-4 years [19] - [25]. The EU's desire to increase the share of renewable energy in the overall energy mix and the legislative changes undertaken stimulate technological development and production of elements, parts, equipment, installations, etc. to produce unconventional energy. This, in turn, has put in the focus of researchers not only the necessary resources for this production, but also the impact it causes on the environment and society.

In the next part of our study, we present the research methodology and through the applied methods of analysis we reveal the critical areas in which the negative effect of renewable energy is manifested.

B. Methodology of the Research

For the purposes of our study, we use a bibliometric analysis of the limited scientific literature addressing the problems of renewable energy. In this way, we will establish the existing development trends in the specific area [29]-[31]. Through the bibliometric approach and keyword co-occurrence analysis, we track the co-occurrence of keywords in the studied population, through which we create networks of knowledge elements [31]. Analysing the citation rate of individual publications, which indicates the number of references to a particular study in other publications [32], we will highlight the leading authors and their research.

We use Scopus as a source of data for our analysis, as the database contains a large volume of publications on renewable energy issues (as of 25.03.2026, the database contains 387,946 documents whose titles, keywords or abstract contain the term "renewable energy"). Our choice is dictated by the fact that Scopus is recognized as the largest database with summaries and citations of peer-reviewed publications on a wide range of topics that may not be available in Web of Science [33]. The advantages of Scopus are also confirmed by [34]-[36], which also conduct bibliometric analysis in the field of unconventional energy sources of publications available in Scopus.

Applying statistical techniques, we extract information about leading researchers and their publications, their citations, as well as the source of this publication activity. We visualize the results through VOSviewer [37], as it allows us to create network maps to establish the existing links between the analysed keywords and development trends [37].

To identify the Scopus publications in which authors address the negative impact of renewable sources, we carried out the following:

- Search strategies – We applied a search for a set of keywords in TITLE-ABS-KEY ("renewable energies" OR "renewable energy" AND "negative environmental impact" OR "negative impact").
- Inclusion and Exclusion Criteria – the inclusion and exclusion criteria introduced by us are in terms of: time range – from 2000 to 2026, therefore earlier publications are excluded; language – we

only include publications in English, the rest are excluded; Relevance of content – we only include publications addressing the negative effects of renewable energy, the rest are excluded. There are no exceptions in terms of territory, country or author.

III. RESULTS

A. Bibliometric Performance analysis

By applying the search strategy and the inclusion and exclusion criteria, we generated a sample of 376 posts. We limited the posts to 371 by removing 5 posts that are not in English. We then reviewed the content of each of the publications, excluding another 294 publications that did not address the negative impact of renewable energy sources. The final sample includes 74 publications focusing on the negative impact of renewable energy on the environment and the socio-economic situation of society.

Data on the distribution of publications by year of publication is presented in Figure 2. The presented data allow us to assert that in recent years there has been a relative increase in interest in the issues of the negative impact of renewable resources.

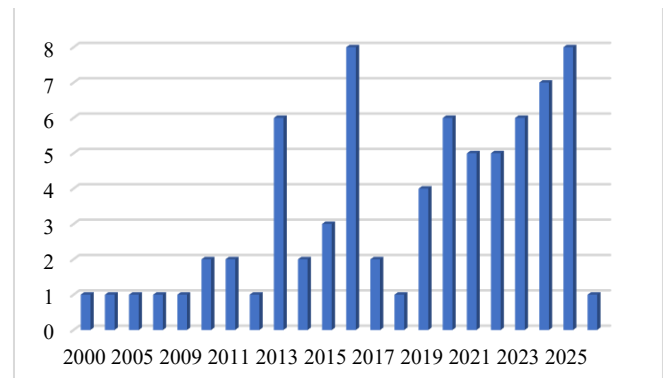


Fig. 2. Number of publications in the period 2000-2026 in Scopus [own calculation, based on Scopus].

The analysis of the publications allows us to establish the number of citations of each author, as well as the publications with the highest citation, which is indicative of the significance and dissemination of these publications among the scientific community (see Table 1).

The information in Table 1 also testifies to the directions of analysis of the authors, and here we can categorically point out that the researchers' interest is focused on the individual sources of renewable energy (photovoltaic systems, wind energy, renewable tidal energy, etc.) and their impact on the environment. It should also be noted here that the citation of the publications is directly dependent on the time factor that is necessary for the dissemination of the author's ideas. This makes the publications of recent years still not report wide distribution among the scientific community.

Analysing the countries from which the selected publications originate, we find that the largest number of documents originate in the United States (8 documents; 717

citations), followed by India (7; 53), Germany (5; 338) and China (5; 131).

The analysis allowed us to argue that research on the negative effect caused by renewable energy sources is partial, fragmented, and insufficient to establish the long-term impact of this type of energy and its sources on the environment. For us, this represents a significant research gap that needs to be filled by broadening and deepening the scope of research in the field.

B. Keywords co-occurrence analysis

To identify the fundamental areas where researchers look for the negative effect of renewable energy, we conducted keywords co-occurrence analysis of the selected studies. To visualize a network map of the relationships between keywords (see Fig. 3), we used VOSviewer, with the analysis in the extracted dataset including “all keywords” in a full count. The total number of generated keywords appearing more than five times reached thirty-three. For each of these words, VOSviewer calculates the strength of the links to the other keywords, and we present the top ten of them in Table 2.

TABLE 1 THE 10 MOST CITED ARTICLES FOR THE PERIOD 2000-2026 IN SCOPUS

Position	Article title	Authors	Total Citations
1	Environmental impacts of solar photovoltaic system: A critical review of recent progress and future outlook	[38]	561
2	Marine Renewable Energy: Potential benefits to biodiversity? An urgent call for research	[39]	380
3	High-level penetration of renewable energy sources into grid utility: Challenges and solutions	[40]	364
4	An integrated DEMATEL-ANP approach for renewable energy sources selection in Turkey	[41]	342
5	Wind farm siting using a spatial analytic hierarchy process approach: A case study of the Städteregion Aachen	[42]	281
6	Near-optimal pi controllers of STATCOM for efficient hybrid renewable power system	[43]	102
7	Fluxes of the greenhouse gases (CO ₂ , CH ₄ and N ₂ O) above a short-rotation poplar plantation after conversion from agricultural land	[44]	96
8	Assessing the effects of wind farms on soil organic carbon	[45]	73
9	Geographical and environmental perspectives for sustainable development of renewable energy in urbanizing China	[46]	73
10	Comparing life cycle implications of building retrofit and replacement options	[47]	72

Considering the information from Table 2, we establish the strongest link between the keywords in terms of the impact of renewable energy on the environment in the context of sustainable development, which is not surprising, since this is the main topic of the analysed publications.

TABLE 2 KEYWORDS CO-OCCURRENCES (2000-2026)

Keyword	Occurrences	Total link strength
environmental impacts	49	221
renewable energy	35	175
sustainable development	25	132
renewable resource	17	86
greenhouse gas	13	86
renewable energy sources	13	42
life cycle	12	68
climate change	11	76
fossil fuel	11	68
life cycle assessment (lca)	11	60

From the network maps (see Fig. 3) we obtain information about the grouping of the highlighted words and the period during which a keyword appeared in the analysed studies.

Visible from the network map of the keywords (see Fig. 3, left), they are grouped into three clusters. *The first red cluster*, which includes “environmental impact” and “environmental protection,” also covers terms related to electrical equipment and efficiency, energy sources, and their life cycle assessment, as well as renewable energy sources such as solar and wind energy, wind farm. *The second green cluster* examines the policies in the field of renewable sources, the economic and social effect they cause, the assessment of their impact on the environment, the relationship with sustainable development and in particular biodiversity and the various aspects of the impact caused by biomass. *The third blue cluster* includes terms relating to biogases and carbon footprint, greenhouse gases, and climate change. The question of land use and fossil fuels is also raised.

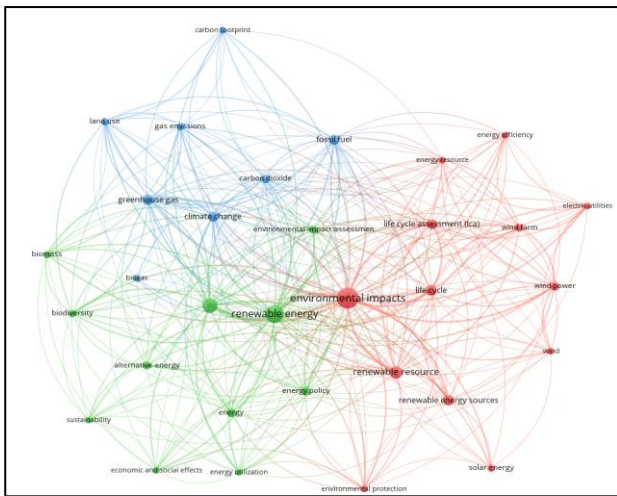


Fig. 3. Keyword Network Visualisation, VOSviewer

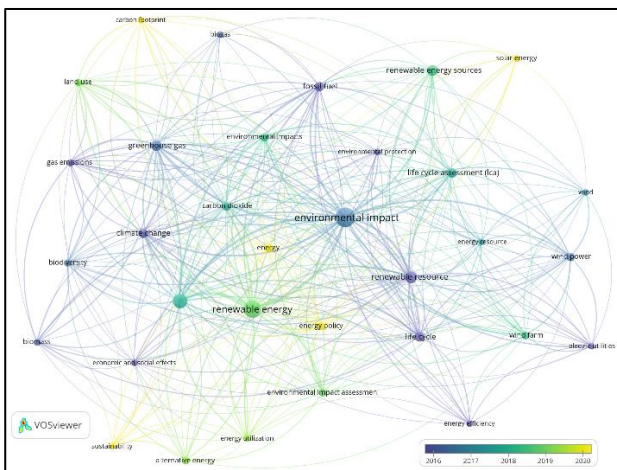


Fig. 4. Keyword Overlay Visualisation, VOSviewer

The right visual map (see Fig. 4) presents us with the same keywords and relationships between them, but we focus on the period of their appearance in the analysed studies, which allows us to highlight the development and trends among researchers. Among the first topics that came to the attention of the authors in the period 2016-2018 are fossil fuels and greenhouse gases causing climate change, energy sources and their efficiency, environmental protection and renewable energy sources such as biomass, biogases, and wind energy. In the period after 2018 to 2020, the focus shifts to assessing the impact of renewables on the environment, land use, sustainability, energy storage options, solar energy, and carbon footprint.

These areas of study reveal a small fraction of the sectors where in-depth analysis is needed to identify the negative impact of renewable energy in the long term and to reveal ways to overcome its negative impacts.

C. Critical Review

The limited number of publications in Scopus that we analysed gave us the starting points for which to deepen our research, including all publications available in online databases (Google Scholar, Science Direct, Web of

Science, Scopus), and the analysis will focus on the negative impact of renewable energy in the following areas: production, use, energy storage, waste, socio-economic consequences.

Production – the production of renewable energy technologies requires the use of scarce raw materials (tellurium and indium – needed for photovoltaics) and rare earth elements (for wind turbines) [48] - [50], the limited global distribution of which raises the question of the relevance and economic appropriateness of extracting such terrestrial resources and how their life cycle can be extended, so that they can be used repeatedly, provided that they are also used in other sectors. More researchers [50] are also paying due attention to environmental pollution caused by the extraction of these rare earth raw materials, as well as to toxic substances released in nature during their use in production [51].

Use – the positioning and use of renewable sources on large land/water areas also causes a negative effect, which is multiplied by considering the various sources of energy. Starting with biomass, whose efficiency and return on energy invested remains low compared to that invested in securing the supply chain [3], here we have the widest recognition among researchers for the adverse effects of its use (loss of biodiversity; groundwater pollution and soil degradation; emits significant carbon emissions when burned; competes with food production and leads to price increases) and at the same time, biomass is actively involved in a number of strategies for the development and expansion of the share of renewable energy [3], [52]. The observed negatives of hydropower are related to impacts on fish populations [39], greenhouse gas emissions from biomass decay under reservoirs, and socio-economic consequences for the population. In the case of solar and wind energy, due to the variability of energy flows, it is necessary to occupy large areas with facilities (photovoltaics and wind turbines) for energy production, which causes deforestation, soil and water pollution, loss of biodiversity, and creates the need to extract ever larger quantities of scarce and rare earth elements [38], [45], [51].

Energy storage – the issue of the capacity and efficiency of renewable energy storage systems, the possibilities for their expansion and reduction of the negative effects arising from their production is also gaining more attention. The expansion of renewable energy sources necessitates an increase in storage capacity and an increase in the production of batteries that require critical minerals. The production process itself has severe consequences for the environment, caused by the transformation of land for mining basins, the outflow of heavy metals, the increase in the amount of industrial waste and wastewater, the depletion of freshwater and salt water, climate change [53].

Waste – the expansion of the application of renewable energy inevitably leads to the generation of large volumes of harmful and hazardous waste, which turn into non-recyclable parts of renewable energy systems. Current research and innovative technologies offer innovative solutions to achieve the recyclability of solar panels, wind

turbine blades, and energy storage batteries [54] - [57], but now the economic efficiency of these processes is below the profitability threshold, therefore it is unattractive for widespread application.

Socio-economic impact – the main socio-economic consequences are related to the extraction of rare earths, which has a negative effect on local communities, due to the depletion of water resources, the destruction of biodiversity, the transformation of agricultural land into renewable energy fields, which affects the most vulnerable groups. In the “Lithium triangle” (Chile, Argentina, Bolivia), the area of extractive basins overlaps with the territories of indigenous peoples, which necessitated his forced eviction. There is also an increased morbidity among the population living in the mining areas.

IV. DISCUSSION AND CONCLUSION

In this study, we do not dispute the importance of renewable energy in modern times as a tool to limit the harmful effects of fossil fuels on the environment. The diversity of renewable energy sources (see Fig. 1) depicts people's abilities to transform natural energy streams into electricity through innovative technologies and facilities. This is also the main direction in the author's research, taking into account the positive effects of renewable technologies [13] – [25] for achieving sustainable development [9] – [12].

At the same time, we firmly defend the position that not every source of energy and not every technology that is used to absorb renewable energy is safe and environmentally friendly. On the contrary, through the analysis of the limited scientific literature, we found that this research area is at the beginning of its development and the long-term effect of renewable energy sources is not sufficiently analyzed. This is confirmed by the Hypothesis derived in this study.

As can be seen from the keywords occurrence analysis (see Table 2), it is 'environmental impact' that is the most common keyword in the analysed set of publications. “Environmental impact” and “environmental protection” are also the keywords around which part of the author's research is focused. Other areas of research are related to the analysis of the life cycle of renewable energy sources and the economic and social effect they cause. In the future, it is necessary to deepen the analysis of the possibilities for reducing the negative impact that the use of renewable technologies generates in the long term, since the cumulative effect leads to a multiplication of the identified and described negatives. Proof in support of our views is the data on the production of photovoltaic (PV) modules, panels and elements (see Fig. 5).

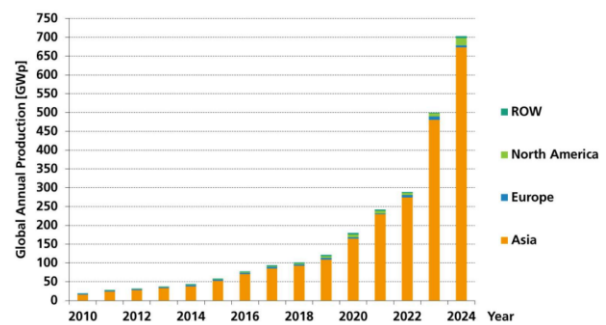


Fig. 5. PV Module Production by Region [58, p.12]

As we find out from Fig. 5, in 2024, nearly 700 GWp of photovoltaic energy is obtained from Asian (in particular Chinese) photovoltaic panels. At the same time, the existing debate about the production of these panels and their parts in plants powered by coal-fired power plants raises the question of how “clean” the electricity produced is. Of course, technological advancements and bringing this issue to the forefront are stimulating Chinese enterprises to switch to using clean energy to produce solar modules, panels, and parts.

In the context of this example, the role of the current study is also manifested – it does not aim to deny the positive side and advantages of renewable energy, but to direct the focus of researchers to the possibilities of increasing the efficiency of renewable energy sources to avoid the already established negative effects.

All the above so far allows us to say that we have fulfilled the purpose of the study by outlining the main thematic areas in which scientific literature investigating the negative effect of renewable energy on the environment is developing. We have listed the publications with the highest citation in Scopus for the period of the study and their authors, who laid the foundation for a research field that should find significant development in the coming years.

According to the prepared critical analysis of the negative effect of renewable energy sources, we offer guidelines in which the efficiency of the use of renewable energy can be improved, including:

- Preparation of a comprehensive analysis of the impact of renewables on the environment and affected groups in the long term.
- Using innovative digital technologies to achieve sustainability [59] and AI-based technologies [60] to increase efficiency in the use of renewable energy, as well as to uncover guidelines to address existing problems.
- Investing in innovative solutions to replace rare earths with more widespread substitutes with the same properties.
- Limiting planned obsolescence and establishing mechanisms to model the innovative obsolescence of renewable energy technologies [61], as well as

investing in innovative recycling practices [54] - [57].

More attention needs to be paid to achieving a balance and harmony between nature and innovative renewable energy solutions, following the example of the “blue economy” [62], rather than pursuing cost-effective but unclear long-term solutions. Taking these criticisms into account can significantly improve the efficiency and appropriateness of expanding the share of renewable energy in the overall energy mix and contribute to stimulating innovative development and competitiveness of industry and SMEs [63] - [64].

The contribution of this research is to outline the problem areas of the development, use and disposal of renewable energy sources, which can serve as a starting point for researchers for further in-depth research and to uncover the possibilities for limiting them. Issues critical for the development of renewable energy are addressed, the solution of which will contribute to achieving a sustainable and balanced development of the energy sector.

Beyond the scope of the current research and subject to future analyses, is the possibility of revealing the negative effects on the environment by individual types of renewable energy sources and highlighting specific guidelines and areas for achieving clean energy, which will contribute to the energy transition and achieving carbon neutrality.

REFERENCES

- [1] L. Bell, “The utilization of natural energy,” in *Cassie’s Magazine*, Vol. 29, 1906, pp. 466–476.
- [2] F.W. Clarke, H.W. Wiley, C.H. Herty, S.W. Parr, R.B. Dole, “Report of the committee of the American chemical society appointed to cooperate with the National Conservation Commission,” in *Science* 29 (745), 1909, pp. 570–574, [Accessed January 10, 2026], DOI: [10.1126/science.29.745.570](https://doi.org/10.1126/science.29.745.570).
- [3] A. Harjanne, J. Korhonen, “Abandoning the concept of renewable energy,” in *Energy Policy*, 127, 2019, pp. 330–340, [Accessed April 10, 2026], <https://doi.org/10.1016/j.enpol.2018.12.029>.
- [4] J. Twidell, *Renewable energy resources*, 4th ed., Routledge: New York, 2021.
- [5] E.T. Sayed, A.G. Olabi, A.H. Alami, A. Radwan, A. Mdallal, A. Rezk, M.A. Abdelkareem, “Renewable Energy and Energy Storage Systems,” in *Energies* 16, 2023, [Accessed December 10, 2025], <https://doi.org/10.3390/en16031415>.
- [6] S. Ahmed, A. Ali, A. D’Angola, “A Review of Renewable Energy Communities: Concepts, Scope, Progress, Challenges, and Recommendations,” in *Sustainability* 16, 2024, [Accessed December 20, 2025], <https://doi.org/10.3390/su16051749>.
- [7] A. Qazi, F. Hussain, N. A. Rahim, G. Hardaker, D. Alghazzawi, K. Shaban, & K. Haruna, “Towards sustainable energy: a systematic review of renewable energy sources, technologies, and public opinions,” in *IEEE access*, 7, 2019, pp. 63837–63851, [Accessed March 12, 2026], DOI: [10.1109/ACCESS.2019.2906402](https://doi.org/10.1109/ACCESS.2019.2906402).
- [8] G.E. Halkos, E.C. Gkampoura, “Reviewing Usage, Potentials, and Limitations of Renewable Energy Sources,” in *Energies* 13, 2020, [Accessed March 2, 2026], <https://doi.org/10.3390/en13112906>.
- [9] P. A. Østergaard, N. Duic, Y. Noorollahi, & S. Kalogirou, “Renewable energy for sustainable development,” in *Renewable energy*, 199, 2022, pp. 1145–1152, [Accessed April 3, 2026], <https://doi.org/10.1016/j.renene.2022.09.065>.
- [10] T. Güney, “Renewable energy, non-renewable energy and sustainable development,” in *International Journal of Sustainable Development & World Ecology*, 26:5, pp. 389–397, [Accessed March 15, 2026], <https://doi.org/10.1080/13504509.2019.1595214>.
- [11] R. Said, M.I. Bhatti, A.I. Hunjra, “Toward Understanding Renewable Energy and Sustainable Development in Developing and Developed Economies: A Review,” in *Energies* 15, 2022, 5349, [Accessed March 20, 2026], <https://doi.org/10.3390/en15155349>.
- [12] R.R. Hernandez, S.M. Jordaan, B. Kaldunski, N. Kumar, “Aligning climate change and Sustainable Development Goals with an innovation systems roadmap for renewable power,” in *Frontiers in Sustainability* 1, 2020, 583090, [Accessed March 20, 2025], <https://doi.org/10.3389/frsus.2020.583090>.
- [13] T. Kabel, M. Bassim, “Literature Review of Renewable Energy Policies and Impacts,” in *European Journal of Marketing and Economics*, Vol. 2, Issue 2, 2019, pp. 28–41, [Accessed March 23, 2026], <https://ssrn.com/abstract=3441105>.
- [14] A. Donastorg, S. Renukappa and S. Suresh, “Financing Renewable Energy Projects in Developing Countries: A Critical Review,” in *IOP Conference Series: Earth and Environmental Science*, 83(1), 2017, 012012, [Accessed March 25, 2026] DOI [10.1088/1755-1315/83/1/012012](https://doi.org/10.1088/1755-1315/83/1/012012).
- [15] Q. Hassan, P. Viktor, T. J. Al-Musawi, B. M. Ali, S. Algburi, H. M. Alzoubi, A. K. Al-Jiboory, A. Z. Sameen, H. M. Salman, M. Jaszczur, “The renewable energy role in the global energy Transformations,” in *Renewable Energy Focus* 48, 2024, 100545, pp.1–16, [Accessed February 25, 2026], <https://doi.org/10.1016/j.ref.2024.100545>.
- [16] H. Garrett-Peltier, “Green versus brown: Comparing the employment impacts of energy efficiency, renewable energy, and fossil fuels using an input-output model,” in *Economic Modelling*, 0–1, 2016, [Accessed July 22, 2025], <https://doi.org/10.1016/j.econmod.2016.11.012>.
- [17] T. Bulavskaya, F. Reynès, “Job creation and economic impact of renewable energy in the Netherlands,” *Renewable Energy*, 119, 2018, pp. 528–538, [Accessed October 26, 2025], <https://doi.org/10.1016/j.renene.2017.09.039>.
- [18] N. Nikolova, D. Petrova, “Investment activity of SMEs in the furniture industry in the Republic of Bulgaria,” in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, vol. 4, June 2025, pp. 251–256, [Accessed March 28, 2026], <https://doi.org/10.17770/etr2025vol4.8436>.
- [19] U. Bulut, “The impacts of non-renewable and renewable energy on CO2 emissions in Turkey,” in *Environmental Science and Pollution Research*, 24(18), 2017, pp. 15416–15426, [Accessed September 28, 2025], <https://doi.org/10.1007/s11356-017-9175-2>.
- [20] M. Makešová, M. Valentová, “The Concept of Multiple Impacts of Renewable Energy Sources: A Critical Review,” in *Energies* 14, 2021, 3183, [Accessed September 26, 2025], <https://doi.org/10.3390/en14113183>.
- [21] A. G. Olabi, M. A. Abdelkareem, “Renewable energy and climate change,” in *Renewable and Sustainable Energy Reviews* 158, 2022, pp. 1–7, [Accessed February 26, 2026], <https://doi.org/10.1016/j.rser.2022.112111>.
- [22] K. Makiela, B. Mazur, J. Głowacki, “The Impact of Renewable Energy Supply on Economic Growth and Productivity,” in *Energies*, 15, 2022, 4808, [Accessed February 26, 2026], <https://doi.org/10.3390/en15134808>.
- [23] B. Khaldia, F. Sadji, B. Riadh, “China Experience in Renewable Energies,” in *J. Manag. Econ. Sci. Prospect* 06, 2022, pp. 700–718.
- [24] N. Ivanova, P. Datta, “The environmental impact of renewable energy,” in *International Journal of Business and Economic Development*, Vol.11, 2023, pp. 85–103.
- [25] M. Wozniak, A. Badora, K. Kud, & L. Wozniak, “Renewable energy sources as the future of the energy sector and climate in Poland – truth or myth in the opinion of the society,” in *Energies*,

- vol. 15, no. 45, 2022, pp. 1-20, [Accessed February 13, 2026], <https://doi.org/10.3390/en15010045>.
- [26] IEA, Renewable energy, 2025. [Online]. Available: International Energy Agency, <https://www.iea.org/energy-system/renewables> [Accessed April 1, 2026].
- [27] A. Q. Al-Shetwi. "Sustainable development of renewable energy integrated power sector: Trends, environmental impacts, and recent challenges," in *Science of The Total Environment*, Vol. 822, 153645, 2022, pp. 1-18, ISSN 0048-9697, [Accessed February 1, 2026], <https://doi.org/10.1016/j.scitotenv.2022.153645>.
- [28] J. Mohtasham, "Renewable energies," in *Energy Procedia*, 74, 2015, pp. 1289-1297, [Accessed February 5, 2026], <https://doi.org/10.1016/j.egypro.2015.07.774>.
- [29] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, W. M. Lim, How to conduct a bibliometric analysis: An overview and guidelines," *Journal of business research*, 133, 2021, pp. 285-296, [Accessed January 13, 2026], <https://doi.org/10.1016/j.jbusres.2021.04.070>.
- [30] I. Passas, "Bibliometric Analysis: The Main Steps," in *Encyclopedia*, 4, 2024, pp. 1014-1025, [Accessed February 5, 2026], <https://doi.org/10.3390/encyclopedia4020065>.
- [31] A. Rejeb, K. Rejeb, I. Zrelli, E. Süle, "Industry 5.0 as seen through its academic literature: an investigation using co-word analysis," in *Discover Sustainability*, 6(1), 2025, 307, [Accessed February 18, 2026], <https://doi.org/10.1007/s43621-025-01166-0>.
- [32] S. Raut, N. U. I. Hossain, M. Kouhizadeh, S. A. Fazio, "Application of artificial intelligence in circular economy: A critical analysis of the current research," in *Sustainable Futures*, 9, 2025, 100784, [Accessed April 1, 2026], <https://doi.org/10.1016/j.sfsr.2025.100784>.
- [33] J. M. Khudhari, J. Kurian, B. Tartakovsky, G. S. V. Raghavan, "Bibliometric analysis of global research trends on microbial fuel cells using Scopus database," in *Biochemical engineering journal*, 136, pp. 51-60, 2018, [Accessed June 02, 2026], <https://doi.org/10.1016/j.bej.2018.05.002>.
- [34] L. Camargo, D. Comas, Y. C. Escorcia, A. Alviz-Meza, G. Carrillo Caballero, I. Portnoy, "Bibliometric Analysis of Global Trends around Hydrogen Production Based on the Scopus Database in the Period 2011–2021," in *Energies*, 16(1):87, 2023, [Accessed June 02, 2026], <https://doi.org/10.3390/en16010087>.
- [35] R. Seminario-Córdova, R. Rojas-Ortega, "Renewable Energy Sources and Energy Production: A Bibliometric Analysis of the Last Five Years," in *Sustainability*, 15(13):10499, 2023, [Accessed June 02, 2026], <https://doi.org/10.3390/su151310499>.
- [36] P. Sharma, A. Sengar, "Trends and insights in renewable energy research: a comprehensive bibliometric analysis (2000–2023)," in *International Journal of Energy Sector Management*, 19(4), 2025, pp. 751–771, [Accessed June 02, 2026], <https://doi.org/10.1108/IJESM-05-2024-0020>.
- [37] N.J. Van Eck, L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," in *Scientometrics*, 84(2), 2010, pp. 523-538, [Accessed March 20, 2025], <https://doi.org/10.1007/s11192-009-0146-3>.
- [38] M. Tawalbeh, A. Al-Othman, F. Kafiah, E. Abdelsalam, F. Almomani, M. Alkasrawi, "Environmental impacts of solar photovoltaic systems: A critical review of recent progress and future outlook," in *Science of the total environment*, 759, 2021, 143528, [Accessed September 26, 2025], <https://doi.org/10.1016/j.scitotenv.2020.143528>.
- [39] R. Inger, M. J. Attrill, S. Bearhop, A. C. Broderick, W. James Grecian, D. J. Hodgson, B. J. Godley, "Marine renewable energy: potential benefits to biodiversity? An urgent call for research," in *Journal of applied ecology*, 46(6), 2009, pp.1145-1153, [Accessed February 26, 2026], <https://doi.org/10.1111/j.1365-2664.2009.01697.x>.
- [40] M. S. Alam, F. S. Al-Ismail, A. Salem, M. A. Abido, "High-level penetration of renewable energy sources into grid utility: Challenges and solutions," *IEEE access*, 8, 2020, pp.190277-190299, [Accessed February 26, 2026], [doi:10.1109/ACCESS.2020.3031481](https://doi.org/10.1109/ACCESS.2020.3031481).
- [41] G. Büyüközkan, S. Güleriyüz, "An integrated DEMATEL-ANP approach for renewable energy resources selection in Turkey," in *International journal of production economics*, 182, 2016, pp. 435-448, [Accessed January 27, 2026], <https://doi.org/10.1016/j.ijpe.2016.09.015>.
- [42] T. Höfer, Y. Sunak, H. Siddique, R. Madlener, "Wind farm siting using a spatial Analytic Hierarchy Process approach: A case study of the Städteregion Aachen," in *Applied energy*, 163, 2016, pp. 222-243, [Accessed April 2, 2026], <https://doi.org/10.1016/j.apenergy.2015.10.138>.
- [43] M. I. Mosaad, H. S. M. Ramadan, M. Aljohani, M. F. El-Naggar, S. S. Ghoneim, "Near-optimal PI controllers of STATCOM for efficient hybrid renewable power system," in *IEEE Access*, 9, 2021, pp. 34119-34130, [Accessed April 19, 2025], [doi:10.1109/ACCESS.2021.3058081](https://doi.org/10.1109/ACCESS.2021.3058081).
- [44] D. Zona, I. A. Janssens, M. Aubinet, B. Gioli, S. Vicca, R. Fichot, R. Ceulemans, "Fluxes of the greenhouse gases (CO₂, CH₄ and N₂O) above a short-rotation poplar plantation after conversion from agricultural land," in *Agricultural and Forest Meteorology*, 169, 2013, pp. 100-110, [Accessed February 1, 2026], <https://doi.org/10.1016/j.agrformet.2012.10.008>.
- [45] O. I. Pekkan, M. A. Senyel Kurkcuoglu, S. N. Cabuk, T. Aksoy, B. Yilmazel, T. Kucukpehlivan,... & M. Cetin, "Assessing the effects of wind farms on soil organic carbon," in *Environmental Science and Pollution Research*, 28(14), 2021, pp. 18216-18233, [Accessed April 1, 2026], <https://doi.org/10.1007/s11356-020-11777-x>.
- [46] C. Bao, C. L. Fang, "Geographical and environmental perspectives for the sustainable development of renewable energy in urbanizing China," in *Renewable and Sustainable Energy Reviews*, 27, 2013, pp. 464-474, [Accessed February 18, 2026], <https://doi.org/10.1016/j.rser.2013.07.008>.
- [47] B. Dong, C. Kennedy, K. Pressnail, "Comparing life cycle implications of building retrofit and replacement options," *Canadian Journal of Civil Engineering*, 32(6), 2005, pp. 1051-1063, [Accessed March 8, 2026], <https://doi.org/10.1139/105-061>.
- [48] N. Kursunoglu, S. Kursunoglu, The Importance of Rare Earth Elements (REEs) for Energy Transition, in 4th International Batman Energy Summit BES'24, 2024, pp. 1-10. [Online]. Available: Research Gate, https://www.researchgate.net/publication/385277875_The_Importance_of_Rare_Earth_Elements_REEs_for_Energy_Transition [Accessed April 1, 2026].
- [49] R. İncekara, "Economic Milestone of the 21st Century: Rare Earth Elements," in *Lectio Socialis*, 9(1), 2025, pp. 151-164, DOI: 10.47478/lectio.1810742, [Accessed April 1, 2026], <https://doi.org/10.47478/lectio.1810742>.
- [50] Y. H. Han, X. W. Cui, Y. Zhang, H. Zhang, Z. Chen, "Environmental impacts of rare earth elements mining and strategies for sustainable management: A comprehensive review," in *Journal of Hazardous Materials*, 2025, 140400, [Accessed April 2, 2026], <https://doi.org/10.1016/j.jhazmat.2025.140400>.
- [51] H.A. Cheema, M. Farhan, H. Kim, "Assessment and Mitigation of Environmental Footprints for Energy-Critical Metals Used in Permanent Magnets," in Pathak, P., Srivastava, R.R., Ilyas, S. (eds) *Anthropogenic Environmental Hazards*. Springer, Cham, 2023, [Accessed September 12, 2025], https://doi.org/10.1007/978-3-031-41013-0_2.
- [52] S. Teske, J. Beranek, S. Tunmore, O. Schaefer, A. Zervos, W. Krewitt, S. Simon, T. Pregger, S. Schmid, W. Graus, E. Blomen, and C. Aubrey, *Energy [r]evolution – A sustainable energy outlook, 4th edition world energy scenario*. Greenpeace International, EREC and GWEC. Netherlands, 2012.
- [53] R. G. Souza, A. M. Domingues, A. Spindlegger, C. Mair-Bauernfeind, F. Part, "Review of the current knowledge and identified gaps in assessing the social and environmental impacts of mining processes in the Lithium Triangle," in *Sustainable Production and Consumption*, 53, 2025, pp. 40-63, [Accessed February 18, 2026], <https://doi.org/10.1016/j.spc.2024.11.031>.
- [54] F. Li, Y. Liu, "Research on New Energy Vehicle Battery (NEV) Recycling Model Considering Carbon Emission," in

- Sustainability. 17(10):4356, 2025, [Accessed February 18, 2026], <https://doi.org/10.3390/su17104356>.
- [55] C. Hao, B. Zhao, X. Guo, S. Zhang, M. Fei, L. Shao, W. Liu, Y. Cao, T. Liu, J. Zhang, "Mild chemical recycling of waste wind turbine blade for direct reuse in production of thermoplastic composites with enhanced performance," in *Resources, Conservation and Recycling*, 215: 108159 2025, [Accessed February 25, 2026], DOI:10.1016/j.resconrec.2025.108159.
- [56] K. H. Ho, A. W. Ee, M. Son, S. Rahmani, F. M. Liyaff & R. Fouquet, "Environmental impact assessment of solar panel production and recycling in Southeast Asia," in *Journal of Cleaner Production*, 522: 146277, 2025. [Accessed February 14, 2026], <https://doi.org/10.1016/j.jclepro.2025.146277>
- [57] L. Li, X. Kang, "Recycling wind turbine blades: A comprehensive review of challenges, solutions, and future directions," in *Journal of Building Engineering*, 114489. 2025, [Accessed February 2, 2026], <https://doi.org/10.1016/j.jobe.2025.114489>
- [58] Fraunhofer ISE, Photovoltaics Report, Freiburg, 31 October 2025 <https://www.ise.fraunhofer.de/en/publications/studies/photovoltaics-report.html>
- [59] N. Nikolova, "Industry 4.0-development and consequences for sustainable development of Bulgaria," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 3, 2021, June, pp. 245-251, [Accessed March 14, 2024], <https://doi.org/10.17770/etr2021vol3.6543>.
- [60] I. Ivanov, K. Petrov, T. Rachovski, D. Petrova, "Methodological and Applied Aspects of Artificial Intelligence in Energy Consumption Prediction," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 2, 2025, June, pp. 165-169, [Accessed January 15, 2026], <https://doi.org/10.17770/etr2025vol2.8601>.
- [61] D. I. Petrova, "An approach to modelling innovation obsolescence," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 1, 2023, June, pp. 175-179, [Accessed September 12, 2025], <https://doi.org/10.17770/etr2023vol1.7237>.
- [62] N. Nikolova, "Entrepreneurial "BLUE" Practices for Sustainable Development and Resources Efficiency," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 1, 2019, June, pp. 198-203, [Accessed March 14, 2026], <https://doi.org/10.17770/etr2019vol1.4114>.
- [63] D. Petrova, N. Nikolova, "Innovative development and competitiveness of the industrial sector in Bulgaria," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 4, 2025, June, pp. 297-304, [Accessed March 14, 2026], <https://doi.org/10.17770/etr2025vol4.8397>.
- [64] V. Boeva, "The Integration of the Digital Economy and the Green Transition—Opportunities for Small and Medium-Sized Enterprises," in *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, Vol. 1, 2025, June pp. 97-102, [Accessed March 30, 2026], <https://doi.org/10.17770/etr2025vol1.8657>.

Capacity and Second-Life Potential of Lithium-Ion Cells Recovered from Disposable E-Cigarettes for Distributed Micro-Energy Storage

Aadu Petrov

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
<https://orcid.org/0009-0003-7628-840X>

Jaak Jõgi

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
<https://orcid.org/0009-0003-6930-2752>

Küllli Hovi

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
kylly.hovi@emu.ee

Andres Annuk

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
<https://orcid.org/0000-0001-5464-0415>

Olga Panova

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
<https://orcid.org/0000-0002-1699-0307>

Mart Hovi

Estonian University of Life Sciences
Institute of Forestry and Engineering
Tartu, Estonia
<https://orcid.org/0009-0001-7175-5895>

Abstract- The widespread adoption of disposable electronic cigarettes has created a rapidly growing waste stream containing embedded lithium-ion batteries. In most cases, these batteries are discarded together with the device once the e-liquid reservoir is depleted, despite the possibility that the electrochemical lifetime of the cell significantly exceeds the functional lifetime of the product. This study investigates the residual capacity and reuse potential of lithium-ion cells recovered from discarded disposable e-cigarettes and evaluates their potential relevance for distributed micro-energy storage applications.

A total of 115 lithium-ion cells were collected from used devices and classified by their standardized cylindrical cell format (e.g., 13300, 14500). Following visual inspection and voltage screening, 102 cells were tested using a standardized constant-current charge-discharge protocol at 0.2C (C-rate) within the voltage range of 4.2-3.0 V. The experimental results show that 87.3% of the tested cells retained more than 85% of their nominal capacity, with an average remaining capacity of 89.8%. Only 3.9% of the tested cells exhibited a remaining capacity below 70%.

These results indicate that a considerable share of lithium-ion batteries discarded with disposable consumer electronics remain technically functional and could be repurposed in low-power applications such as IoT devices, educational platforms, and small distributed storage modules. The findings highlight the importance of systematic collection, classification and diagnostic approaches for small-format lithium-ion batteries in order to support circular economy principles and reduce unnecessary loss of critical battery materials.

Keywords - battery diagnostics, circular economy, nano distributed energy storage, state of health

I. INTRODUCTION

The rapid growth of disposable electronic cigarettes has introduced a new stream of lithium-ion battery waste. These devices are typically discarded once the e-liquid is depleted, although the embedded batteries often remain electrochemically functional. This mismatch between product lifetime and battery lifetime represents a significant inefficiency. This study investigates the residual capacity of such batteries and evaluates their potential for second-life applications in sustainable energy systems.

II. BACKGROUND AND RELATED WORK

A. Lithium-Ion Battery Degradation and State of Health

Lithium-ion batteries are widely used in portable electronics due to their high energy density, low self-discharge rate, and relatively long cycle life. However, their performance degrades over time due to a combination of electrochemical and mechanical processes [1-2]. The primary ageing mechanisms include the formation and growth of the solid electrolyte interphase layer on the anode, structural degradation of electrode materials, and loss of active lithium inventory. These processes lead to a gradual reduction in available capacity and an increase in internal resistance over the battery lifetime.

Battery condition is commonly described using the concept of State of Health (SoH), which is typically defined

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.47>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

as the ratio of the current capacity to the nominal capacity of a new cell. In practical applications, capacity retention is one of the most widely used indicators of battery health, particularly in cases where detailed electrochemical diagnostics are not available. Previous studies [3-4] have shown that lithium-ion batteries can retain a significant portion of their initial capacity even after extended use, depending on operating conditions such as temperature, charge-discharge rates, and depth of discharge.

In small consumer devices, including disposable electronic cigarettes, batteries are often operated under relatively moderate conditions, which may limit the extent of degradation. As a result, a considerable fraction of such batteries may remain in good electrochemical condition at the time of disposal.

B. Lithium-Ion Batteries in Disposable Consumer Electronics

The rapid growth of disposable electronic devices has introduced a new category of lithium-ion battery waste. Disposable e-cigarettes represent a particularly relevant example, as they integrate a lithium-ion cell into a single-use product whose operational lifetime is determined primarily by the consumption of e-liquid rather than by battery degradation.

Typical batteries used in disposable e-cigarettes have nominal capacities in the range of approximately 300-1000 mA·h and operate at nominal voltages around 3.7 V. Despite their relatively small size, these cells are fully functional electrochemical energy storage devices, often comparable in performance to rechargeable cells used in other portable electronics.

Previous studies have shown that a large proportion of such batteries retain a high fraction of their nominal capacity at the time of disposal. This observation is further supported by the experimental results presented in this study. In that study, most tested cells exhibited capacity retention above 85%, suggesting that their electrochemical lifetime significantly exceeds the functional lifetime of the host device. This mismatch between product lifetime and battery lifetime represents a key inefficiency in current consumption patterns.

C. Second-Life Batteries and Circular Economy

The concept of second-life batteries has gained increasing attention as a strategy to improve resource efficiency and reduce environmental impact. Second-life applications involve repurposing batteries after their initial use, typically in less demanding applications where reduced performance is acceptable [5].

Most research on second-life batteries has focused on large-format lithium-ion batteries, particularly those used in electric vehicles. After their automotive use, such batteries are often repurposed for stationary energy storage applications, where requirements for power and performance are less stringent.

In contrast, relatively limited attention has been paid to the second-life potential of small-format lithium-ion batteries from consumer electronics. However, the

increasing volume of such devices suggests that they may represent a non-negligible resource, particularly when considered in aggregate.

From a circular economy perspective, extending the useful life of batteries reduces the need for raw material extraction and decreases the environmental burden associated with battery production and disposal. Even small batteries may contribute to material efficiency if collected, tested and reused systematically [6].

D. Distributed Nano-Energy Storage Systems

The transition towards more decentralized energy systems has increased interest in distributed energy storage, including small-scale and modular storage solutions. While most distributed storage systems are based on relatively large battery units, there is growing interest in nano-scale storage for applications such as IoT devices, sensor networks, and low-power autonomous systems.

Although individual small-format batteries provide limited energy, large numbers of such cells could theoretically be aggregated into distributed storage systems. This concept is analogous to virtual power plants, where many small resources are combined to provide system-level functionality.

In this context, recovered lithium-ion cells from disposable devices could represent a potential resource for experimental or niche applications in distributed micro-energy storage. However, practical implementation requires reliable methods for battery screening, classification and safety assurance [7].

E. Research Gap

While lithium-ion battery degradation and second-life applications have been extensively studied in the context of large-scale energy storage, there is a lack of experimental data on the condition and reuse potential of small-format batteries recovered from disposable consumer electronics [8].

This study addresses this gap by providing experimental data on the residual capacity of lithium-ion cells extracted from disposable e-cigarettes and evaluating their potential role in second-life applications within sustainable energy systems.

III. MATERIALS AND METHODS

A. Sample Collection and Preparation

The experimental dataset consisted of 115 lithium-ion cells recovered from discarded disposable electronic cigarettes. The devices were collected through voluntary contributions during the period September to December 2024.

Only cells that met the following criteria were included in the sample:

- clearly identifiable battery format markings,
- intact safety membranes,

- no visible mechanical deformation, corrosion, or leakage.

Cells exhibiting physical damage or safety risks were excluded from the study.

The disassembly of e-cigarette devices was performed manually using insulated tools to prevent short circuits. Each battery was carefully removed from the device housing and labelled with a unique identification number ranging from 1 to 115. The entire disassembly process was conducted in accordance with standard electronic waste handling safety procedures, including the use of protective eyewear and non-conductive work surfaces.

The distribution of battery formats in the collected sample is shown in Fig. 1.



Fig. 1. Collected samples.

B. Battery Types

The collected sample included several commonly used lithium-ion cell formats: (Fig. 19

- 13300 format - 51 cells (44.3%),
- 14500 format - 20 cells (17.4%),
- 13350 format - 20 cells (17.4%),
- other formats - 24 cells (20.9%).

The two most common formats (13300 and 14500) accounted for 61.7% of the total sample, which is consistent with typical disposable e-cigarette device configurations.

C. Experimental Setup

Battery capacity measurements were performed using a 150 W DC electronic load-based battery tester, capable of controlling discharge current and cutoff voltage while recording the discharge profile and total capacity in milliampere-hours (mA·h).

All experiments were conducted under controlled laboratory conditions:

- temperature: 20 ± 2 °C,

- relative humidity: 40-60%.

These conditions were maintained to ensure measurement consistency, as battery performance is known to be temperature-dependent.

The experimental setup is illustrated in Fig. 2.

D. Testing Procedure

The testing protocol consisted of four main stages.

1) Initial Inspection and Voltage Screening

Each cell was visually inspected, and its initial voltage was measured using a digital multimeter. Cells with an initial voltage below 3.2 V were excluded from further testing due to safety concerns related to deep discharge and potential instability during recharging.

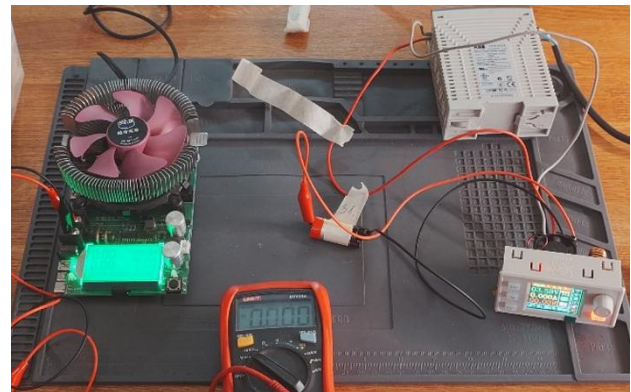


Fig. 2. Experimental setup.

A total of 13 cells were excluded at this stage and classified as untested.

2) Charging

The remaining 102 cells were charged using a constant current-constant voltage (CC-CV) method. Charging was performed using an XY6509S DC-DC converter powered by an ABB CP-E 24/2.5 power supply.

The charging current was set to 0.2C, which is a standard moderate-rate charging condition for lithium-ion cells. Here, 1C (C-rate) corresponds to a current equal to the nominal capacity of the cell (in A), resulting in a full charge or discharge in one hour. At a discharge rate of 0.2C, the charge process lasted approximately five hours, assuming nominal capacity. The maximum charging voltage was 4.2 V.

3) Discharging and Capacity Measurement

After charging, the cells were discharged using an ATORCH 150 W electronic load tester under controlled conditions.

Discharge parameters:

- discharge current: 0.2C (C-rate),
- voltage range: 4.2 V to 3.0 V.

During discharge, the tester recorded the voltage profile and calculated the total delivered capacity in milliampere-hours (mA·h).

4) Capacity Retention and Classification

The remaining capacity of each cell was calculated by comparing the measured capacity to the nominal capacity specified for the battery.

Capacity retention was expressed as:

$$\text{Capacity retention} = \frac{C_{\text{measured}}}{C_{\text{nominal}}} \cdot 100$$

Based on the calculated values, the cells were classified into five categories:

- Very good / new: 95-100%
- Good: 85-94%
- Moderate: 70-84%
- Poor: 50-69%
- Failed: <50%

All measurement results were recorded and stored in a dataset for further statistical analysis.

IV. RESULTS AND DISCUSSION

Out of the total 115 collected lithium-ion cells, 102 cells (88.7%) were successfully tested, while 13 cells (11.3%) were excluded due to low initial voltage (below 3.2 V). These excluded cells were classified as untested for safety reasons. The fact that only 11.3% of collected cells were excluded due to low voltage further supports the observation that most batteries are discarded before reaching end-of-life conditions.

The tested cells exhibited a consistently high level of capacity retention. The majority of cells-87.3% (89 cells)-retained at least 85% of their nominal capacity. Only 8.8% (9 cells) showed moderate capacity (70-84%), and 3.9% (4 cells) were classified as poor (50-69%). No cells with capacity below 50% were observed. The average remaining capacity was 89.8%, with a median of 91.4%, indicating that most discarded cells remain in good electrochemical condition.

A comparison of battery formats revealed relatively consistent performance across different cell types. The most common format, 13300, showed an average capacity retention of 90.6%, with 89.1% of cells classified as good. The 14500-format demonstrated similarly stable performance, with 90% of cells in good condition and an average capacity of 89.1%. The 13350-format exhibited slightly greater variability, with 77.8% of cells classified as good and an average capacity of 86.8%.

Other battery formats also showed generally good performance, with no cells falling into the lowest capacity category. Across all formats, the average capacity retention ranged between 86.8% and 90.6%, confirming

that most batteries are discarded while still retaining a substantial portion of their usable capacity.

These results highlight a mismatch between the functional lifetime of disposable e-cigarettes and the electrochemical lifetime of their batteries. While the devices are discarded after the e-liquid is depleted, the batteries often remain in good condition. This suggests significant potential for second-life applications, particularly in low-power systems such as IoT devices or small-scale distributed energy storage.

From a sustainability perspective, the premature disposal of functional lithium-ion batteries represents a loss of valuable materials. Improved collection, testing, and reuse strategies could support more efficient resource utilization and contribute to circular economy principles.

V. CONCLUSIONS

This study evaluated the condition and reuse potential of lithium-ion cells recovered from disposable e-cigarettes. Out of 115 collected cells, 102 were successfully tested, and the results showed consistently high-capacity retention. A total of 87.3% of tested cells retained more than 85% of their nominal capacity, with an average remaining capacity of 89.8%, indicating that most cells remain in good electrochemical condition at the time of disposal.

The results confirm a clear mismatch between the functional lifetime of disposable devices and the electrochemical lifetime of their batteries. Despite being discarded, the majority of cells still retain a substantial fraction of their usable capacity.

The findings suggest that these cells have potential for second-life applications, particularly in low-power and distributed micro-energy systems. While individual cells provide limited energy, their large-scale aggregation may represent a novel resource for experimental and niche energy applications.

From a sustainability perspective, the premature disposal of functional lithium-ion batteries represents a loss of valuable materials. Improved collection, classification, and reuse strategies could support more efficient resource utilization and contribute to circular economy principles.

REFERENCES

- [1] A. Barré et al., "A review on lithium-ion battery ageing mechanisms and estimations for automotive applications," *Journal of Power Sources*, vol. 241, pp. 680-689, 2013. DOI: 10.1016/j.jpowsour.2013.05.040
- [2] M. Bercibar et al., "Critical review of state of health estimation methods of Li-ion batteries for real applications," *Renewable and Sustainable Energy*

Reviews, vol. 56, pp. 572-587, 2016. DOI: 10.1016/j.rser.2015.11.042

[3] E. Martinez-Laserna et al., "Battery second life: Hype, hope or reality? A critical review of the state of the art," *Renewable and Sustainable Energy Reviews*, vol. 93, pp. 701-718, 2018. DOI: 10.1016/j.rser.2018.04.035

[4] L. C. Casals, B. A. Garcia, and F. Aguesse, "Second life of electric vehicle batteries: Relation between materials degradation and environmental impact," *Journal of Cleaner Production*, vol. 145, pp. 337-345, 2017.

[5] X. Luo, J. Wang, M. Dooner, and J. Clarke, "Overview of current development in electrical energy storage technologies and the application potential in power system operation," *Applied Energy*, vol. 137, pp. 511-536, 2015.

[6] G. Harper et al., "Recycling lithium-ion batteries from electric vehicles," *Nature*, vol. 575, pp. 75-86, 2019.

[7] D. Deng, "Li-ion batteries: basics, progress, and challenges," *Energy Science & Engineering*, vol. 3, no. 5, pp. 385-418, 2015.

[8] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: A top-down survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1040-1065, 2014.

[9] J. B. Goodenough and K.-S. Park, "The Li-ion rechargeable battery: a perspective," *Journal of the American Chemical Society*, vol. 135, no. 4, pp. 1167-1176, 2013.

Comparative Analysis of Efficiency and Economic Performance of a Dual-Fuel Diesel Engine Fueled with Compressed Natural Gas and Hydrogen

Atanasi Tashev

*Transport and Aircraft Equipment and Technologies
Department*

*Technical University of Sofia, Branch Plovdiv
Center of Competence "Smart Mechatronic, Eco- and
Energy-Saving Systems and Technologies"*

4000 Plovdiv, Bulgaria
atanasi.tashev@tu-plovdiv.com

Evgeni Dimitrov

*Department of Combustion Engines, Automobile Engineering
and Transport*

*Technical University of Sofia
Sofia, Bulgaria
etzd@tu-sofia.bg*

Abstract—This study presents a comparative experimental analysis of the thermodynamic and economic performance of a compression ignition engine operating in conventional diesel mode and in dual-fuel mode with compressed natural gas and hydrogen. The investigation evaluates the influence of gaseous fuel addition on fuel consumption, brake specific fuel consumption, thermal efficiency, and cost of energy production under identical operating conditions. Experimental tests were conducted on a single-cylinder diesel engine at constant engine speed of 2000 min^{-1} and variable load, using both fixed ($K = 20\%$) and maximum gas substitution ratios. The performance of the engine was assessed based on measured fuel consumption parameters and calculated efficiency indicators. An economic evaluation was also performed using representative fuel prices. The results show that conventional diesel operation achieves the highest thermal efficiency, reaching approximately 29.5% at medium load, compared to about 28 – 29% for hydrogen and 26 – 27% for compressed natural gas. From an economic perspective, compressed natural gas provides the lowest cost of energy production, reaching values as low as approximately 0.50 €/kWh, followed by diesel at around 0.65 – 0.70 €/kWh, while hydrogen results in the highest cost, exceeding 1.0 €/kWh at low loads due to its higher fuel price. The results highlight a clear trade-off between efficiency and cost. While diesel operation remains the most efficient, and compressed natural gas is the most economically favorable option, hydrogen demonstrates improved performance compared to methane and offers significant environmental benefits.

Keywords— *compressed natural gas, dual-fuel engine, hydrogen, thermal efficiency.*

I. INTRODUCTION

Internal combustion engines (ICEs) continue to play a dominant role in transportation, agriculture, and distributed power generation systems due to their robustness, high energy density, and operational flexibility. Among the various types of ICEs, compression ignition (CI) engines are particularly valued for their superior thermal efficiency and durability. However, the increasing demand for reduced environmental impact and improved energy efficiency has led to intensified research efforts toward the utilization of alternative fuels and advanced combustion strategies [1] – [5].

One of the most promising approaches to achieving these objectives is the implementation of dual-fuel combustion, commonly referred to as the gas–diesel cycle. In this mode of operation, a gaseous fuel is introduced into the intake air, forming a premixed charge that is ignited by a pilot injection of diesel fuel. This method allows partial substitution of conventional diesel fuel while maintaining stable combustion and engine operability. The dual-fuel concept provides an opportunity to simultaneously influence combustion characteristics, fuel economy, and exhaust emissions, depending on the type and proportion of the gaseous fuel used [6], [7].

Compressed natural gas (CNG), with methane as its primary component, is one of the most widely investigated gaseous fuels for dual-fuel applications. Its relatively low cost, widespread availability, and established infrastructure make it an attractive option for practical implementation. Studies have shown that the use of CNG in dual-fuel CI engines can lead to a reduction in carbon dioxide and

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol3.113>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

particulate emissions due to its lower carbon-to-hydrogen ratio compared to diesel fuel [8] - [10]. Furthermore, at higher engine loads, improved combustion conditions contribute to enhanced thermal efficiency and reduced specific fuel consumption.

Despite these advantages, several limitations of CNG-diesel operation have been identified. At low and medium loads, the slower flame propagation speed of methane and the reduced in-cylinder temperature can lead to incomplete combustion, resulting in increased emissions of carbon monoxide (CO) and unburned hydrocarbons (HC).

Additionally, the displacement of intake air by gaseous fuel may reduce the available oxygen for combustion, further contributing to inefficiencies under certain operating conditions [11], [12]. These challenges highlight the importance of optimizing operating parameters such as load, gas substitution ratio, and injection strategy.

Hydrogen (H_2) has attracted considerable attention as a next-generation alternative fuel due to its unique physicochemical properties. It is a carbon-free fuel with a significantly higher lower heating value (LHV) compared to hydrocarbon fuels, wide flammability limits, and high flame speed. These properties enable rapid and more complete combustion, which can improve thermal efficiency and reduce carbon-based emissions. Moreover, hydrogen's high diffusivity promotes better mixing with air, leading to a more homogeneous charge and enhanced combustion stability, particularly at lean conditions.

Experimental studies have demonstrated that hydrogen enrichment in dual-fuel CI engines can lead to reduced brake specific fuel consumption and improved overall engine efficiency [13], [14]. Additionally, significant reductions in exhaust gas opacity and carbon dioxide emissions have been reported due to the absence of carbon in hydrogen fuel. However, the use of hydrogen is also associated with certain challenges. The higher combustion temperatures and faster heat release rates may result in increased nitrogen oxide (NO_x) emissions, particularly at higher engine loads. Furthermore, hydrogen's low density can reduce volumetric efficiency, affecting the overall air-fuel mixture formation [15], [16].

The dual-fuel concept has also been explored with other gaseous fuels, such as liquefied petroleum gas (LPG), which has demonstrated similar trends in enhancing combustion intensity and increasing in-cylinder pressure. These findings confirm that the introduction of a gaseous fuel into the diesel combustion process fundamentally alters the thermodynamic and kinetic characteristics of the cycle, providing opportunities for performance optimization.

Although a substantial body of research exists on dual-fuel engines, most studies focus primarily on emission characteristics or performance parameters independently. Comparative analyses between different gaseous fuels are often limited to specific aspects, such as emissions behavior, without a comprehensive evaluation of efficiency and economic performance under identical operating conditions. This creates a gap in the current literature,

particularly in understanding the trade-offs between thermodynamic benefits and economic feasibility.

In practical applications, the economic aspect of fuel utilization is of critical importance. While methane is relatively inexpensive and supported by established infrastructure, hydrogen remains significantly more costly due to production, storage, and distribution challenges. Therefore, evaluating the cost of energy production in addition to engine efficiency is essential for determining the real-world applicability of dual-fuel strategies.

Based on the above considerations, the primary objective of the present study is to perform a comparative experimental assessment of the influence of compressed natural gas and hydrogen addition on the performance and economic characteristics of a compression ignition engine operating in dual-fuel mode under conventional diesel engine settings. The investigation is conducted at identical operating conditions and constant gas substitution ratios, allowing direct comparison of the effects of the two gaseous fuels on fuel consumption, thermal efficiency, and cost of energy production.

The study is focused on practical dual-fuel implementation scenarios, where existing diesel engines operate without substantial modification of their original design and calibration parameters. Such an approach reflects many currently applied dual-fuel systems used in practice, where gaseous fuels are introduced into conventionally calibrated diesel engines in order to simplify implementation and reduce conversion complexity.

It should be emphasized that the present work does not aim to optimize the combustion process separately for each gaseous fuel. Parameters such as injection timing, compression ratio, and fuel delivery strategy are intentionally maintained close to the standard diesel configuration in order to evaluate the direct influence of fuel substitution under comparable baseline conditions. Future investigations will focus on dedicated optimization of dual-fuel combustion parameters for hydrogen and methane operation.

II. MATERIALS AND METHODS

For the experimental investigation, a single-cylinder compression ignition engine type DV550 was used. The engine is characterized by a cylinder bore of $D = 91.5$ mm, a piston stroke of $S = 85$ mm, and a compression ratio of $\epsilon = 17.5$. The engine operates with direct fuel injection and has a rated brake power output of 8 kW at a rotational speed of $n = 3000$ min⁻¹. The injection timing angle was kept as its default setting of 20° before top dead center for all of the operation modes.

The test engine is coupled to a direct current electric dynamometer (SAK 28), which enables precise control of the engine load and measurement of brake performance parameters. The dynamometer is capable of absorbing power up to 28 kW at engine speeds reaching 6000 min⁻¹, thus ensuring stable operation over a wide range of test conditions.

The experimental setup is designed to allow operation in dual-fuel mode, where gaseous fuel (compressed natural gas or hydrogen) is introduced into the intake manifold. The gas is supplied in a pulsed manner through solenoid-controlled valves. The *CNG* injection pressure was in range between 0.85 to 0.9 bar while the H_2 pressure was in the range 0.3 to 0.59 bar. The injection duration and, consequently, the mass flow rate of the gaseous fuel are regulated by a dedicated electronic control unit (*ECU*). The control system was specifically developed at the Department of Combustion Engines, Automobile Engineering and Transport, Technical University of Sofia, and allows flexible adjustment of the gas supply parameters.

The determination of gaseous fuel consumption is based on measurements of volumetric flow, pressure, and temperature. A diaphragm-type gas flow meter (*G4*) is used in combination with a pressure gauge and a type *K* thermocouple to determine the operating conditions of the supplied gas. The temperature range of *CNG* gas fuel and H_2 is in the range of 18 – 21.5 °C and 26.5 – 28 °C correspondingly. The measured volumetric flow is converted into mass flow using the corresponding thermodynamic relations. The maximum relative uncertainty associated with the determination of the hourly gaseous fuel consumption is estimated to be 8.2%.

The consumption of the liquid diesel fuel is determined using a custom-developed volumetric flow measurement system. The method is based on recording the time required for the engine to consume a predefined volume of fuel, allowing the calculation of the corresponding mass flow rate. The measured time was in the between 23 and 67 sec. This approach provides reliable measurement of fuel consumption under steady-state operating conditions. The maximum relative uncertainty of the diesel fuel consumption measurement is evaluated at 6.9%.

A schematic representation of the experimental setup, including the fuel supply systems, measurement instrumentation, and dynamometer arrangement, is presented in Fig. 1.

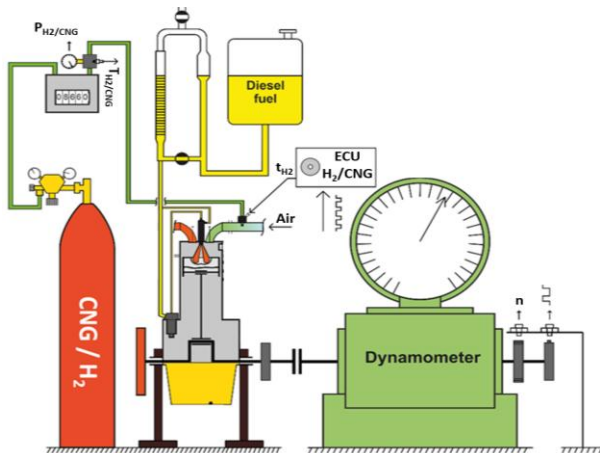


Fig. 1. Test setup

The quantity of gaseous fuel supplied to the engine is characterized by the coefficient *K*. This parameter defines the mass share of the gaseous fuel relative to the total fuel consumption and can be expressed as:

$$K = \frac{B_{gas}}{B_h} 100, \% \quad (1)$$

where B_{gas} is the hourly consumption of gaseous fuel, kg/h, and B_h represents the total (combined) hourly fuel consumption, kg/h.

The total fuel consumption is determined as the sum of the gaseous and liquid fuel components:

$$B_h = B_{gas} + B_D, \text{ kg/h} \quad (2)$$

where B_D is the hourly diesel fuel consumption, kg/h.

The hourly fuel consumption used to calculate the brake specific fuel consumption – b_e :

$$b_e = \frac{B_h}{N_e}, \text{ kg/kWh} \quad (3)$$

where N_e is the engine brake power, kW.

The engine thermal efficiency (η_e) is calculated based on the following equation:

$$\eta_e = \frac{3,6 \cdot 10^3}{\left[(LHV_D \left(1 - \frac{K}{100} \right) + LHV_{gas} \frac{K}{100}) \cdot b_e \right]} \cdot 100, \% \quad (4)$$

where LHV_D and LHV_{gas} are the low heat values of the diesel fuel (~42.5 MJ/kg) and gas fuel (~120 MJ/kg for H_2 and ~49.1 MJ/kg for *CNG*) respectively.

In addition to the thermodynamic evaluation, an economic analysis was performed in order to assess the cost effectiveness of the dual-fuel operation. The economic performance of the engine was evaluated based on the cost of produced energy, expressed in €/kWh.

The cost of energy production - C_{kWh} was calculated using the specific fuel consumption and the corresponding fuel prices according to the following relationship:

$$C_{kWh} = b_e \left[\left(1 - \frac{K}{100} \right) P_D + \frac{K}{100} P_{gas} \right] \quad (5)$$

where P_D and P_{gas} are the corresponding fuel price, of the diesel and gas fuels €/kg.

The fuel prices used in the analysis were selected based on representative market values and are assumed constant for the purpose of comparison. This approach enables a consistent evaluation of the economic impact of methane and hydrogen addition under identical operating conditions.

The experimental results used for comparing the effects of *CNG* and H_2 on engine thermal efficiency and economic analysis were obtained at constant values of the coefficient *K* ($K = 20\%$ and $K = \text{max}$) and variable engine loads (load characteristics), while maintaining a constant engine speed of $n = 2000 \text{ min}^{-1}$. The engine load point used for the test are expressed by brake mean effective pressure equal to: 0.22 MPa (30% load), 0.31 MPa (47% load), 0.375 MPa (57% load) and 0.436 MPa (67% load). These results are based on previously determined regulating characteristics.

The regulating characteristics are defined under conditions of constant engine load, expressed by constant brake mean effective pressure ($p_e = \text{const}$), and variable values of the coefficient K ($K = \text{var}$). Additional details regarding the experimental methodology and the procedure for obtaining these characteristics are provided in [6], [17].

The maximum admissible share of gaseous fuel supplied to the engine ($K = \text{max}$) is determined based on the onset of limiting operating conditions. These include either a critical rate of in-cylinder pressure rise or the occurrence of misfire, which may result from an excessively small pilot diesel quantity with insufficient energy to initiate reliable combustion of the gas–air mixture.

In the present study, a value of $K = 20\%$ was selected as a representative operating point, ensuring stable engine operation and allowing a consistent comparison between the different gaseous fuels.

III. RESULTS AND DISCUSSION

The experimental results obtained from the investigation of the dual-fuel diesel engine operation with methane (*CNG*) and hydrogen (*H₂*) are presented in Fig. 2 to Fig. 5. The analysis focuses on the influence of the gaseous fuel type and substitution ratio on fuel consumption, brake specific fuel consumption, thermal efficiency, and cost of energy production.

A. Hourly Fuel Consumption

At $K = 20\%$ (Fig. 2a), the total hourly fuel consumption exhibits a similar increasing trend with load for all investigated fuel modes. The introduction of gaseous fuels leads to variations in total consumption depending on their physicochemical properties. Hydrogen-assisted operation generally results in lower total fuel consumption compared to *CNG*, particularly at lower loads, which can be attributed to its higher energy content and faster combustion characteristics.

However, when compared to conventional diesel operation, the differences are less pronounced and vary with load. Diesel operation demonstrates competitive fuel consumption, especially at higher loads, where combustion conditions are more favorable. In contrast, *CNG* operation tends to exhibit slightly higher consumption values across the load range, particularly at low loads, due to slower flame propagation and incomplete combustion.

At $K = \text{max}$ (Fig. 2b), the reduction in total fuel consumption with hydrogen becomes more noticeable, especially at low and medium loads. Nevertheless, the comparison with diesel operation indicates that the benefits of gaseous fuel substitution are strongly dependent on operating conditions and substitution ratio, rather than representing a uniform improvement.

The increase in total fuel consumption observed during dual-fuel operation can be explained by several factors associated with the combustion process in gas–diesel mode. The introduction of gaseous fuel into the intake manifold displaces part of the intake air, which may reduce

volumetric efficiency and affect the air–fuel ratio inside the cylinder. In addition, the combustion process becomes strongly dependent on the interaction between the diesel pilot injection and the premixed gaseous fuel–air mixture.

For methane operation, the relatively low flame propagation speed and lower reactivity of the fuel may lead to incomplete combustion, particularly at low loads and high gas substitution ratios. In the case of hydrogen, combustion is more intensive due to its high flame speed and wide flammability limits; however, the non-optimized combustion phasing and standard diesel engine calibration may still prevent full utilization of the fuel energy. As a result, the dual-fuel process may lead to increased overall fuel consumption and reduced thermal efficiency compared to optimized conventional diesel operation.

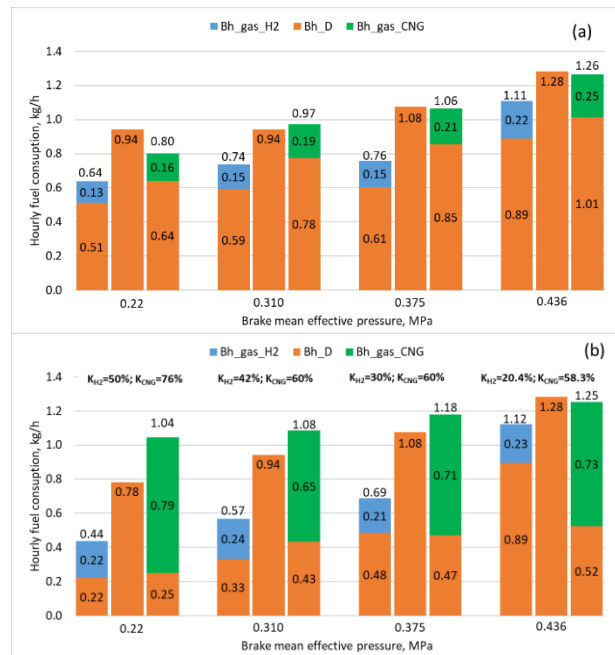


Fig. 2. Variation of total hourly fuel consumption as a function of brake mean effective pressure at (a) constant gas substitution ratio ($K = 20\%$) and (b) maximum admissible substitution ($K = \text{max}$).)

B. Brake Specific Fuel Consumption

At $K = 20\%$ (Fig. 3a), the lowest brake specific fuel consumption values are observed during conventional diesel operation across the entire load range. The introduction of gaseous fuels leads to an increase in b_e , reflecting less efficient overall energy conversion in dual-fuel mode.

Among the investigated gaseous fuels, hydrogen demonstrates lower B_e values compared to *CNG*, indicating more favorable combustion characteristics and improved utilization of the supplied energy relative to methane. However, despite this improvement, hydrogen-assisted operation does not reach the efficiency level of pure diesel combustion. For example, at $p_e = 0.375$ MPa, the b_e value for hydrogen remains higher than that of diesel, while still being significantly lower than that of *CNG*.

At $K = \max$ (Fig. 3b), the differences between the fuels become more pronounced. *CNG* exhibits the highest b_e values, particularly at low loads, where incomplete combustion effects are dominant. Hydrogen operation shows improved performance compared to *CNG*, with reduced specific consumption, but still remains less efficient than diesel operation. This behavior confirms that while hydrogen enhances combustion relative to methane, the dual-fuel process inherently introduces limitations compared to conventional diesel combustion.

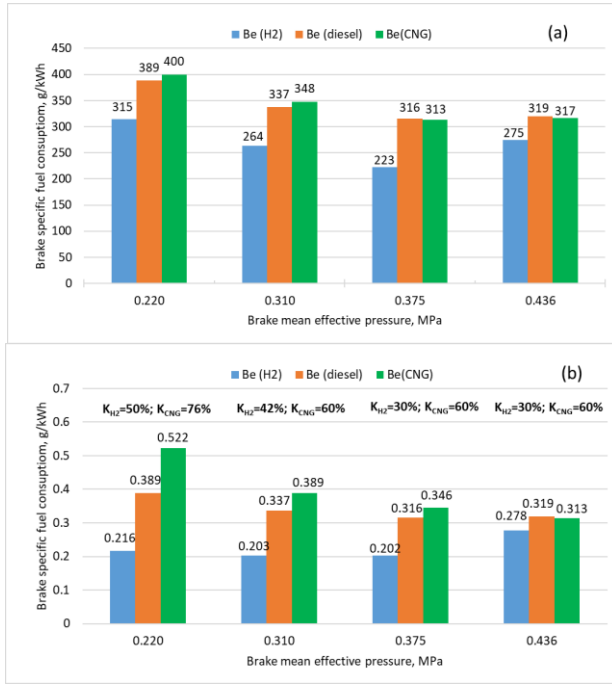


Fig. 3. Brake specific fuel consumption versus brake mean effective pressure for diesel, *CNG*, and hydrogen dual-fuel operation at (a) $K = 20\%$ and (b) $K = \max$.)

C. Thermal Efficiency

The thermal efficiency calculations are based on the total supplied fuel energy, including both the diesel pilot fuel and the gaseous fuel contribution. The variation of η_e is presented in Fig. 4.

At $K = 20\%$ (Fig. 4a), conventional diesel operation demonstrates the highest thermal efficiency across most of the investigated load range. The introduction of gaseous fuels results in a reduction in efficiency, which is more pronounced in the case of *CNG*. Hydrogen-assisted operation shows improved efficiency compared to *CNG*, particularly at medium and high loads, due to its favorable combustion properties such as high flame speed and wide flammability limits.

However, despite these advantages, hydrogen does not exceed the efficiency of diesel operation. This can be explained by the inherent characteristics of dual-fuel combustion, including reduced volumetric efficiency and less optimal ignition conditions compared to direct diesel injection.

At $K = \max$ (Fig. 4b), the efficiency differences between the fuels become more evident. *CNG* exhibits a significant decrease in efficiency at low loads, indicating poor combustion stability. Hydrogen maintains intermediate efficiency values, consistently higher than those of *CNG* but still below diesel operation. At higher loads, the gap between the fuels decreases, suggesting improved combustion conditions for all modes.

Overall, the results indicate that while hydrogen improves efficiency relative to methane, conventional diesel operation remains the most efficient mode under the investigated conditions.

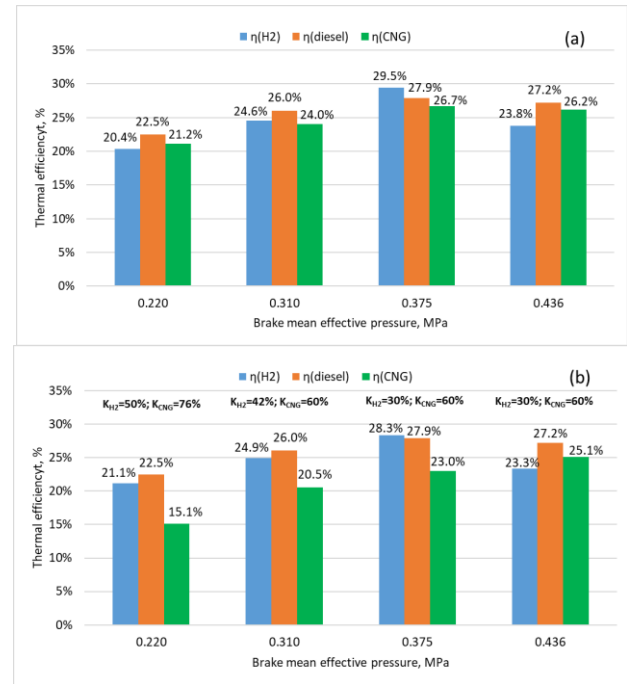


Fig. 4. Brake thermal efficiency (based on the total supplied fuel energy, including both the diesel pilot fuel and the gaseous fuel contribution) as a function of engine load for different fuel configurations at (a) constant substitution ratio ($K = 20\%$) and (b) maximum substitution level ($K = \max$.)

D. Cost of Energy Production

The economic analysis results are presented in Fig. 5, showing the cost of energy production (€/kWh).

At $K = 20\%$ (Fig. 5a), *CNG* provides the lowest cost of energy across all operating points, followed by diesel, while hydrogen remains significantly more expensive. For example, at $p_e = 0.375$ MPa, the cost is approximately 0.61 €/kWh for *CNG*, 0.68 €/kWh for diesel, and 0.74 €/kWh for hydrogen.

This trend is consistent across all loads and reflects the relatively high market price of hydrogen compared to conventional fuels.

At $K = \max$ (Fig. 5b), the cost difference becomes even more pronounced. Despite the improved efficiency, hydrogen operation results in the highest cost of energy, reaching values above 1.0 €/kWh at low loads. In contrast,

CNG achieves the lowest cost (as low as 0.50 €/kWh), making it the most economically favorable option.

Considering the current fuel prices used in the present study, hydrogen operation remains economically less favorable compared to CNG-assisted dual-fuel combustion. However, the economic competitiveness of hydrogen is strongly dependent on future reductions in production, storage, and distribution costs. Based on the obtained results, hydrogen could become economically comparable to CNG if its market price decreases substantially below the currently assumed value of approximately 8 €/kg. Such a scenario is considered realistic in the context of ongoing development of green hydrogen technologies and expansion of hydrogen infrastructure.

In addition, it should be noted that many currently implemented dual-fuel retrofit systems in practical applications operate without dedicated optimization of engine calibration parameters for gaseous fuels. Despite this limitation, such systems remain attractive due to their relatively simple implementation and reduced conversion costs.

It should also be noted that the investigated dual-fuel operation modes were implemented using the standard diesel engine calibration settings, without dedicated optimization for each gaseous fuel. Under such conditions, increases in total fuel consumption and reductions in thermal efficiency may occur due to several factors, including reduced volumetric efficiency, altered ignition characteristics, non-optimal combustion phasing, and incomplete oxidation of the premixed gaseous fuel-air mixture. These effects are particularly pronounced at low loads and high gas substitution ratios.

Despite these limitations, the applied methodology reflects many practically implemented retrofit dual-fuel systems currently used in stationary and transport applications, where preservation of the original diesel engine configuration is preferred due to lower cost and reduced system complexity.

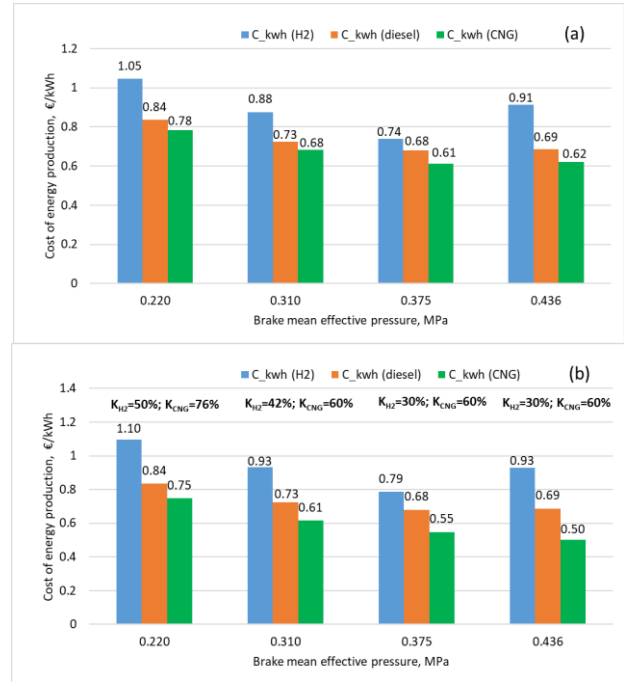


Fig. 5. Cost of energy production (€/kWh) as a function of brake mean effective pressure for diesel, CNG, and hydrogen operation at (a) $K = 20\%$ and (b) $K = \max$.)

IV. CONCLUSIONS

A comparative experimental study of a compression ignition engine operating in conventional diesel mode and in dual-fuel mode with methane (CNG) and hydrogen (H_2) was conducted. The analysis covered fuel consumption, brake specific fuel consumption, thermal efficiency, and cost of energy production under identical operating conditions.

The results show that conventional diesel operation remains the most efficient mode in terms of thermal efficiency across the investigated load range. The introduction of gaseous fuels leads to a slight reduction in efficiency, which is more pronounced in the case of methane. Hydrogen-assisted operation demonstrates better efficiency compared to CNG; however, it does not surpass the efficiency of pure diesel operation. This behavior can be explained by changes in mixture formation and combustion characteristics in dual-fuel mode, including reduced volumetric efficiency and altered ignition conditions.

A similar trend is observed for brake specific fuel consumption. The lowest values are achieved in diesel-only operation, while the addition of gaseous fuels results in an increase in specific fuel consumption. Among the dual-fuel modes, hydrogen shows lower b_e values compared to CNG, indicating more efficient combustion relative to methane, although still inferior to conventional diesel operation.

In terms of hourly fuel consumption, hydrogen operation demonstrates lower total fuel consumption compared to both diesel and CNG dual-fuel modes under certain operating conditions, particularly at lower loads. This effect is associated with the high energy content of

hydrogen and its favorable combustion kinetics. *CNG* operation generally results in higher fuel consumption, especially at low loads, due to slower combustion and incomplete oxidation of the fuel–air mixture.

From an economic perspective, conventional diesel operation and *CNG* dual-fuel mode offer more favorable results compared to hydrogen. The cost of energy production for hydrogen remains the highest among the investigated fuels, primarily due to its elevated market price. In contrast, *CNG* provides the lowest cost per unit of produced energy, making it the most economically viable option under current conditions. Diesel operation shows intermediate cost values, depending on the load.

It should be emphasized that the economic evaluation is based on a hydrogen price of approximately 8 €/kg. Although hydrogen is currently not a cost-competitive fuel, significant reductions in its price are expected in the future as production technologies and infrastructure develop. Under such conditions, hydrogen could become a promising alternative, combining acceptable efficiency with substantial environmental advantages.

In addition to the economic considerations, hydrogen offers important ecological benefits due to its carbon-free nature, which reduce the majority of harmful emissions. These characteristics position hydrogen as a perspective long-term solution for sustainable engine operation.

Overall, the results indicate that while conventional diesel operation remains superior in terms of efficiency, and *CNG* represents the most economically attractive alternative, hydrogen shows potential as a cleaner fuel with improved performance compared to methane. Its wider application will strongly depend on future reductions in fuel cost and further optimization of dual-fuel combustion strategies.

Future research will focus on optimization of the dual-fuel combustion process for the individual gaseous fuels. Particular attention will be given to parameters such as diesel pilot injection timing, compression ratio, gaseous fuel injection strategy, and combustion phasing in order to improve thermal efficiency and overall engine performance under hydrogen- and methane-assisted operation.

ACKNOWLEDGMENTS

This research was funded by the European Regional Development Fund within the OP “Research, Innovation and Digitalization Programme for Intelligent Transformation 2021–2027”, Project No. BG16RFPR002-1.014-0005 Center of competence “Smart Mechatronics, Eco- and Energy Saving Systems and Technologies”

REFERENCES

- [1] R. Miletiev, I. Damyanov, E. Iontchev and R. Yordanov, "Smart in-vehicle environment monitoring system," 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 2020, pp. 1-4, doi: [10.1109/ET50336.2020.9238166](https://doi.org/10.1109/ET50336.2020.9238166)
- [2] K. Ambarev, V. Nikolov and A. Ivanov, "System of experimental study of diesel engine at work with Brownian gas," *Mechanics of the Machines*, vol. 115, pp. 20–23, 2016.
- [3] G. Mladenov, I. Damyanov, D. Saliev and E. Iontchev, "Design of measurement system for vehicle emissions in real road conditions," in *Proceedings of the 30th National Conference with International Participation 'Telecom 2022'*, Sofia, Bulgaria, 2022, pp. 1–4.
- [4] G. D. Mladenov, I. Damyanov, D. N. Saliev, T. Valkovski, M. Radev, "Measurement of vehicle emissions in real road conditions part II," *Results and analysis. AIP Conf. Proc.* 24 January 2024; 2980 (1): 050007. <https://doi.org/10.1063/5.0186011>
- [5] A. Dimitrov, "Alternative fuels in ICE—solutions and problems," *Machine Technology and Materials*, vol. 1-2007, pp. 54–64, 2007.
- [6] E. Dimitrov, A. Tashev and S. Pantchev, "Methodology for experimental investigation of the influence of gaseous fuels on the performance of the diesel engine operating on gas-diesel cycle," in *Proceedings of BulTrans-2015, Sozopol*, Bulgaria, 2015, pp. 103–107.
- [7] V. Nguyen, S. Nayak, H. Le, J. Kowalski, B. Deepanraj, X. Duong, T. Truong, V. Tran, D. Cao and P. Nguyen, "Performance and emission characteristics of diesel engines running on gaseous fuels in dual-fuel mode," *International Journal of Hydrogen Energy*, vol. 49, pp. 868–909, 2024. <https://doi.org/10.1016/j.ijhydene.2023.09.130>
- [8] M. S. Lounici, K. Loubar, L. Tarabet, M. Bilistrou, D. C. Niculescu and M. Tazerout, "Towards improvement of natural gas-diesel dual fuel mode: An experimental investigation on performance and exhaust emissions," *Energy*, vol. 64, pp. 200–211, 2014. <https://doi.org/10.1016/j.energy.2013.10.049>
- [9] R. Papagiannakis and T. Hountalas, "Combustion and exhaust emission characteristics of a dual fuel compression ignition engine operated with pilot diesel fuel and natural gas," *Energy Conversion and Management*, vol. 45, pp. 2971–2987, 2004. <https://doi.org/10.1016/j.enconman.2004.01.013>
- [10] G. Belgiorno, G. Di Blasio and C. Beatrice, "Parametric study and optimization of the main engine calibration parameters and compression ratio of a methane-diesel dual fuel engine," *Fuel*, vol. 222, pp. 821–840, 2018. <https://doi.org/10.1016/j.fuel.2018.02.038>
- [11] J. C. Egusquiza, S. L. Braga and S. Braga, "Performance and gaseous emissions characteristics of a natural gas/diesel dual fuel turbocharged and aftercooled engine," *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, vol. 31, pp. 142–150, 2009.
- [12] J. Liu, F. Yang, H. Wang, M. Ouyang and S. Hao, "Effects of pilot fuel quantity on the emissions characteristics of a *CNG*/diesel dual fuel engine with optimized pilot injection timing," *Applied Energy*, vol. 110, pp. 201–206, 2013. <https://doi.org/10.1016/j.apenergy.2013.04.012>
- [13] K. Debnath, K. Saha and N. Sahoo, "Effect of hydrogen-diesel quantity variation on brake thermal efficiency of a dual fuelled diesel engine," *Journal of Power Technologies*, vol. 92, pp. 55–67, 2012.
- [14] E. Dimitrov, B. Gigov, S. Pantchev, P. Michaylov and M. Peychev, "A study of hydrogen fuel impact on compression ignition engine performance," in *MATEC Web of Conferences*, vol. 234, 03001, 2018. <https://doi.org/10.1051/mateconf/201823403001>
- [15] T. Tsujimura and Y. Suzuki, "The utilization of hydrogen in hydrogen/diesel dual fuel engine," *International Journal of Hydrogen Energy*, vol. 43, pp. 14019–14029, 2018. <https://doi.org/10.1016/j.ijhydene.2018.06.105>
- [16] Y. Karagöz, İ. Güler, T. Sandalcı, L. Yüksek and A. Dalkılıç, "Effect of hydrogen enrichment on combustion characteristics, emissions and performance of a diesel engine," *International Journal of Hydrogen Energy*, vol. 41, pp. 656–665, 2016. <https://doi.org/10.1016/j.ijhydene.2015.11.012>
- [17] E. Dimitrov, A. Tashev, M. Peychev and E. Pavlova, "Methodologies for conducting experimental studies related to the application of gaseous fuels in internal combustion engines," *Journal of Physics: Conference Series*, 3099 (1), art. no. 012004, 2025, <https://doi.org/10.1088/1742-6596/3099/1/012004>