Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 231-238

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

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.

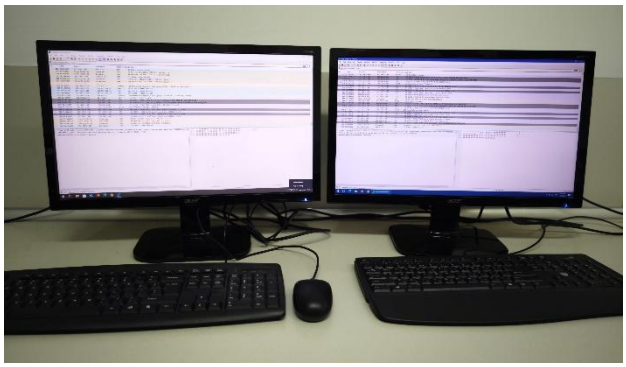

Fig. 1. Computer-based high-risk technical system.

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].

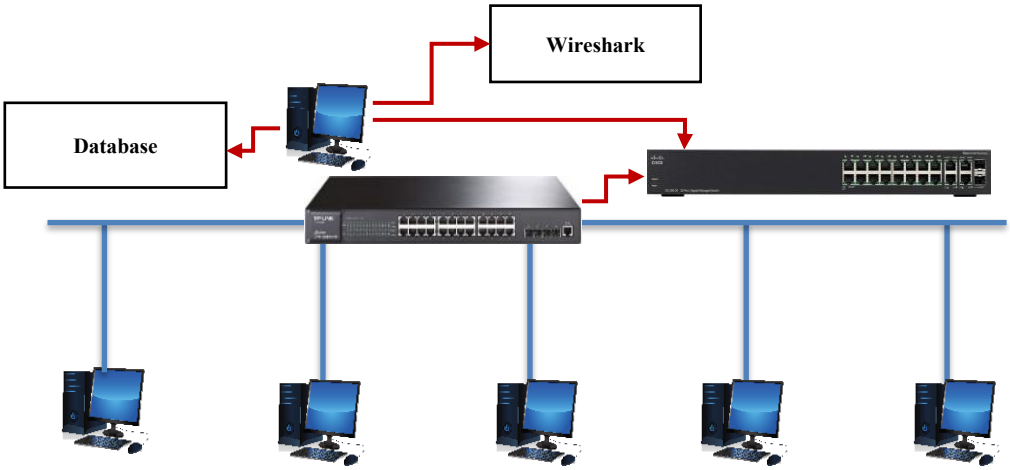

Fig. 2. Structural diagram with personal computers configuration.

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

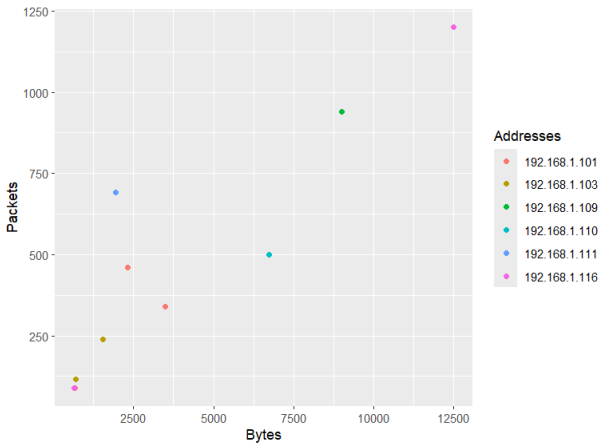

Fig. 3. Scatter plot of the data density after network-wide improvement.

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.

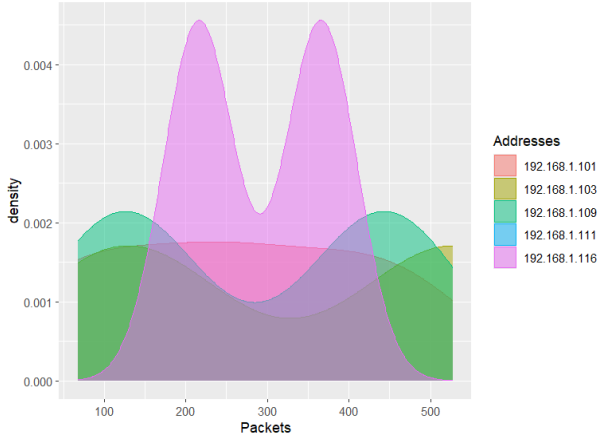

Fig. 4. Kolmogorov-Smirnov plot of the data density after network-wide improvement.

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].

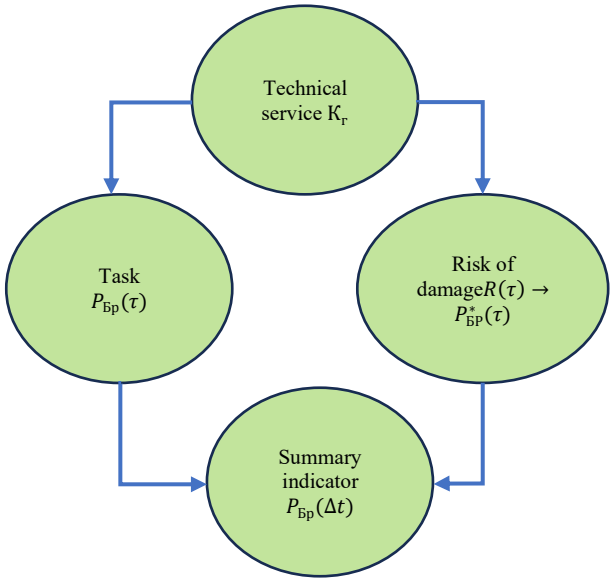

Fig. 5. PC maintenance and operation model.

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:

$$P_{Бр}(\Delta t) = K_r(\Delta t).P_{Бр}(\tau).P_{Бр}{}^*(\tau) \quad (1)$$

where: $\mathbf{P_{Бр}(\Delta t)}$ is the basic probability of failure-free operation during maintenance of personal computers for a time interval $\boldsymbol{\Delta t}$ which can be for a certain period of time in this case 1 year, determined by statistical analysis;

$\mathbf{K_r(\Delta t)}$ - is the primary availability factor of personal computers, mathematically calculated based on the mean time to failure for the 1-year period $\mathbf{T_0}$ and the average time to recovery after failure again for 1 year $\mathbf{T_B}$;

$\mathbf{P_{Бр}(\tau)}$ - is the probability of basic uptime for a certain average period of time for performing a given task $\boldsymbol{\tau}$ (for a device is $\boldsymbol{\tau = 1h}$, for personal computer $\boldsymbol{\tau = 4\ h}$);

$\mathbf{P_{Бр}{}^*(\tau)}$ - is the total probability of failure-free operation, including the factor of catastrophic functional failures and technical failures for an average period of operation $\boldsymbol{\tau}$. 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 $\boldsymbol{\tau(h)}$ and is determined by the formula:

$$P_{Бр}(\tau) \approx 4 - \frac{\tau}{T_0} = 4 - \varpi(\tau).\tau \quad (2)$$

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:$\boldsymbol{\varpi}_{ЛА}(\mathbf{h})$ 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 $\boldsymbol{\tau}(\mathbf{h})$. The mathematical statistics for multiple failures depict reliable and robust results for personal computer PC3, where $\mathbf{P}_{Бр}(\boldsymbol{\tau}) = \mathbf{0.896}$ at $\boldsymbol{\tau} = \mathbf{4\ h}$, based on the large number of reserved mathematical control operations for calculation and processing. Personal computer PC5 reaches after one year of technical operation $\mathbf{P}_{Бр}(\boldsymbol{\tau}) = \mathbf{0.88}$ at $\boldsymbol{\tau} = \mathbf{10\ h}$. 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 $\mathbf{P}_{Бр}(\boldsymbol{\tau})$. Based on the mean time between hardware failures $\mathbf{T_H}$, the availability factor $\mathbf{K}_Г$, the basic mean time to recover from failure $\mathbf{T_B}$, the average intensity of failure times $\boldsymbol{\varpi}(\mathbf{t})$ for 1 year and the basic probability of failure-free operation $\mathbf{P}_{Бр}(\boldsymbol{\tau})$ 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 $\boldsymbol{\tau} = \mathbf{1,5\ h}$. The average time between two failures in the computer network, leading to the need to change the main execution plan, is $\mathbf{T_0} = \mathbf{1,5\ h}$. From equation 2 $\mathbf{P}_{Бр}(\boldsymbol{\tau}) = \mathbf{0.95}$ is determined at $\boldsymbol{\delta} < \mathbf{0.0114}$. 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 $\boldsymbol{\tau}$, is calculated by equation:

$$P_{Бр}{}^*(\tau) = 1 - R(\tau).Q(K/O) \quad (4)$$

where: $\mathbf{R}(\boldsymbol{\tau})$ – is the possible risk of catastrophic functional failure of the personal computer for task processing time $\boldsymbol{\tau}$; $\mathbf{Q}(\mathbf{K/O})$ - 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 $\mathbf{R}(\boldsymbol{\tau})$, where $\boldsymbol{\tau}$ represents the total processing time of tasks by the PC over a calendar time interval $\boldsymbol{\Delta t} = \mathbf{1\ year}$. The overall conditional probability of mismatch in the occurrence of special emergency situations during processing is denoted as $\boldsymbol{\psi}_{\mathbf{R}}(\boldsymbol{\tau})$ and is also determined relative to the total time $\boldsymbol{\tau}$ of the PC for the calendar period $\boldsymbol{\Delta t} = \mathbf{1\ year}$. 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 $\mathbf{R}(\boldsymbol{\tau})$ and $\boldsymbol{\psi}_{\mathbf{R}}(\boldsymbol{\tau})$ are presented in Table 4. Likewise, the same table provides the time $\mathbf{T}_{ОСП}$, 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}
$T_{ОСП}$	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 $\mathbf{Q}(\mathbf{K/O})$, 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:

$$R(\tau) = 10^{-2}; Q(K/O)1.10^{-1}; P_{Бр}{}^*(\tau) = 0.88759 \quad (6)$$

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 ($\Delta t = 1\,year$) — the allowable probability of failure-free operation $\mathrm{P_{Бр.ДОП}}(\Delta t)$, during core operation and with a minimum initial availability factor $\mathrm{K_{Г,min}} = 0.74$ for PC, is calculated using the formula:

$$P_{\text{Бр.ДОП}}(\Delta t) = K_{\Gamma,min}.\, P_{\text{Бр}}{}^{*}(\tau).\, P_{\text{Бр}}(\tau) = exp\left[-\omega_{\text{ДОП}}.\, t_{\Sigma\text{ЛЕ}i}\right] \quad (7)$$

where: $\mathbf{t_{\Sigma ЛЕi}}$ - is the total amount of time for a given PC to operate for the time interval $\mathbf{\Delta t}$; $\boldsymbol{\omega}_{\text{ДОП}}$ - is the total allowable value of the intensity relative to the maximum number of failures ω(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 $\boldsymbol{\omega}_{\text{ДОП}}$, by utilizing the assumption of relative constancy of $\boldsymbol{\omega}_{\text{ДОП}}$ within the observation intervals $\mathbf{\Delta t}$ 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: $\mathbf{P_{Бр.ДОП}}(\mathbf{\Delta t}) \geq \mathbf{0,65231}$. 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: $\mathbf{P_{Бр.ДОП}}(\mathbf{\Delta t}) \geq \mathbf{0,6032}$. For a main comparison, we can also refer to the computer system with an installed PC2, whose reliability indicators are:

$$K_{\Gamma,min} = 0.65\,,\ P_{\text{Бр}}{}^{*}(\tau) = 0.632\,, P_{\text{Бр}}(\tau) = 0.064\,, \mathrm{P_{БР_{ДОП}}}(1\text{ г.}) = 0.677 \quad (8)$$

We can additionally add as well another computer system with an installed PC1, where its reliability indicators are:

$$\mathrm{K_{\Gamma,min}} = 0.75\,,\ \mathrm{P_{Бр}}{}^{*}(\tau) = 0.559\,, \mathrm{P_{Бр}}(\tau) = 0.155\,, \mathrm{P_{БР_{ДОП}}}(1\text{ г.}) = 0.589 \quad (9)$$

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).

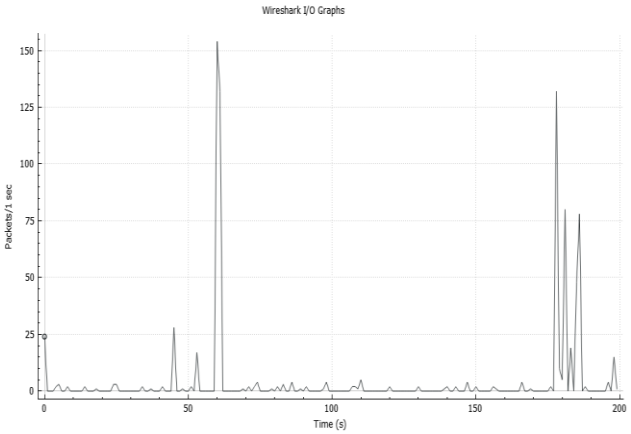

Fig. 6. Reliability analysis of vulnerable technical systems post network enhancements.

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:

$$P_r(t) = K_r \times P_u(t) \times P_{task}(t) \quad (10)$$

where K_r is the availability factor, $P_u(t)$ is the basic probability of failure-free operation, and $P_{task}(t)$ 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:

$$F_{AI}(t) = 1 - \hat{R}(t),\ \ 0 < F_{AI}(t) \leq 1 \quad (12)$$

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.