Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 399-407

Integrated Risk Assessment Model for Cyber Threats to Critical Infrastructure

Irena Petrova
Dept of Technology, Organization and Management of Transport
Todor Kableshkov University of Transport, Sofia, Bulgaria
ipetrova@vtu.bg
ORCID: 0009-0001-6321-7210

Kostadin Trifonov
Dept of Technology, Organization and Management of Transport
Todor Kableshkov University of Transport, Sofia, Bulgaria
ktrifonov@vtu.bg
ORCID: 0000-0002-9130-483X

***Abstract*—Critical infrastructure has become increasingly vulnerable to complex cyber threats characteristic of the contemporary hybrid security environment. The convergence of digital attacks, information operations, and potential physical disruptions necessitates integrated risk assessment approaches that capture both technological and operational dimensions of infrastructure systems. This study presents an integrated risk assessment model for cyber threats targeting critical infrastructure, combining artificial intelligence (AI) techniques with expert transport-system analysis, with a specific focus on railway infrastructure as a key component of national security. The proposed model comprises: (1) an AI-based anomaly detection module; (2) probabilistic hybrid-threat modeling; and (3) a transport-logistics resilience assessment. Simulation results demonstrate higher accuracy in risk prediction, earlier detection of critical deviations, and more effective planning of protective measures. The model supports identifying the most vulnerable infrastructure elements and developing adaptive response strategies.**

Keywords—critical infrastructure, cybersecurity, hybrid threats, railway systems.

I. INTRODUCTION

Railway infrastructure has maintained strategic significance in national security for over a century. Railways remain essential for the movement of people, goods, and military assets. The increasing deployment of digital control systems has further elevated the sector's importance while expanding its vulnerability to hostile interference [1], [2].

Critical infrastructure (CI) represents the backbone of national security, economic security, and social functioning [3]. Increasing digitalization, automation, and interconnectivity have expanded the attack surface of CI systems [4]. Modern cyberattacks take the form of hybrid operations that combine cyber intrusions, misinformation, and physical disruptions, simultaneously leveraging vulnerabilities across technological, operational, and organizational layers. The global railway cybersecurity market reflects this urgency: valued at USD 8.0 billion in 2024, it is projected to reach USD 16.0 billion by 2033, growing at a CAGR of 7.98% [5], while concurrent estimates indicate a compound annual growth rate of 8.62% through 2032 [6].

Railway systems are particularly exposed due to their reliance on signaling and interlocking systems, communication networks, SCADA-based energy subsystems, and tightly coupled operational processes [7]. Even short-term disruptions might propagate rapidly, causing cascading delays, safety risks, and operational degradation. The consequences go beyond the railway sector itself, carrying deep implications for national security and public welfare.

Conventional risk assessment frameworks were built around single-vector threats; they systematically underestimate scenarios in which cyber intrusion, physical sabotage, and disinformation operate in sequence [8], [9], [10]. Measuring and quantifying cybersecurity performance is itself a major challenge: as Brotby and Hinson [11] demonstrate, effective cybersecurity metrics must be both SMART and PRAGMATIC — specific, measurable, actionable, and time-dependent — to support meaningful decision-making. Machine learning methods can detect deviations in control-system behaviour within seconds — a response window that manual monitoring cannot match [12]. Continuous monitoring alone is insufficient: without automated response logic, anomaly detection flags events too late for human operators to intervene before cascading failures propagate [13]. Purpose-built cybersecurity risk assessment software further supports this by automating risk register maintenance, quantifying threat impact, and guaranteeing alignment with frameworks such as NIST CSF and ISO 27001 [14].

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.134

This study introduces an integrated risk assessment model that incorporates AI-based anomaly detection, probabilistic hybrid threat modeling, and transport logistics resilience analysis. The model facilitates vulnerability identification, prediction of cascading failures, and improved operational continuity in the context of hybrid threats.

II. Literature Review on The Research Topic

Research on cyber-physical security has expanded substantially over the past decade, motivated by the increasing complexity, interconnectivity, and digitalization of critical infrastructure systems. Foundational surveys such as Humayed et al. [3] and Flammini [15] emphasize that modern cyber-physical systems (CPS) exhibit tightly coupled operational, communication, and control layers, in which disruptions in one domain rapidly propagate to others. For sectors such as rail and energy — where a 15-minute outage can trigger national-level consequences — this interdependence makes CPS security a first-order engineering problem, not a compliance exercise.

The shift from isolated intrusions to coordinated hybrid operations is now well-documented. Early analyses of industrial cyber incidents — most notably the Stuxnet case examined by Karnouskos [8] — demonstrated that cyberattacks can directly cause physical consequences. More recent studies, such as those by Rass et al. [16] and Hahn et al. [17], show that adversaries increasingly combine cyber intrusions, physical sabotage, and information manipulation to amplify their impact. Hybrid threat modeling structures, therefore, incorporate probabilistic reasoning, attack graph analysis, and scenario-driven simulation to model nonlinear escalation patterns [9], [18]. The inherent nature of these threats is not confined to railways but extends across all digitized transport domains. In the maritime sector, GPS and AIS spoofing attacks have escalated sharply, with over 1,000 vessels per day reportedly affected by signal interference in the Persian Gulf and Strait of Hormuz [19]. At the same time, government-backed actors have targeted port logistics, classification societies, and ship communications [20]. In aviation, a pro-Russian hacktivist group, Killnet, executed a sustained DDoS offensive against EUROCONTROL in April 2023, disrupting the European air traffic management agency's communication systems and forcing airlines onto backup procedures [21]; earlier, researchers demonstrated that legacy ACARS and ADS-B protocols could be exploited to manipulate aircraft navigation data with few barriers [22]. In the space domain, the most consequential documented attack occurred on 24 February 2022, one hour before Russia invaded Ukraine, when Russian GRU actors deployed AcidRain wiper malware against Viasat's KA-SAT satellite network, turning off tens of thousands of modems across Ukraine and Europe, causing the malfunction of 5,800 wind turbines in Germany, and disrupting Ukrainian military command and control [23]. Finally, penetration testing of public EV charging infrastructure has revealed analogous vulnerability surfaces — availability disruption, data manipulation, and authentication bypass [13], [24] — confirming that cyber-physical vulnerabilities follow consistent cross-sector patterns across all interconnected transport and energy systems.

Within the transport domain, railway systems have become a critical focus area due to their reliance on signaling, interlocking, communication networks, and SCADA-based energy subsystems. Yilmaz et al. [7] and Ghafouri et al. [25] document the growing vulnerability of railway signaling systems to cyber intrusions, noting that even short-duration disruptions might trigger cascading operational failures. Maranco et al. [26] further demonstrate that intelligent transportation systems are increasingly exposed to communication interference, GNSS spoofing, and coordinated cyber-physical attacks. These data emphasize the need for consolidated security systems that account for both cyber and operational dimensions of railway infrastructure. Ibadah, Benavente-Peces, and Pahl [27] further extend this analysis to on-board and trackside sensor networks, cataloging protocol-level vulnerabilities in MVB and CAN communications and proposing a multi-tiered security architecture for railway cyber-physical systems. The transition to the Future Railway Mobile Communication System (FRMCS) introduces additional identity management and access-control requirements that further expand the attack surface of digitalized railway networks, necessitating service-oriented security architectures aligned with the evolving FRMCS specification [28].

Artificial intelligence has become a central element of modern intrusion detection and cyber-physical monitoring. Machine learning-based anomaly detection techniques — including SVMs, Recurrent neural networks, autoencoders, and unsupervised outlier detection — have been shown to outperform traditional expert systems in detecting subtle irregularities in CPS behavior [29]. Wang et al. [30] and Tuaama [12] further demonstrate that deep learning models can detect temporal and organizational patterns in industrial control data, enabling earlier detection of malicious activity. These AI-powered approaches are increasingly being applied in transport management systems as part of broader digitalization efforts [31]. Systematic mapping studies further confirm the growing deployment of AI across offensive and defensive cybersecurity scenarios — including detection, automated response, and threat intelligence applications [32].

Resilience research complements cybersecurity studies by examining how infrastructure systems absorb, adapt to, and recover from disruptions. Flammini [15] and Z. Wang, X. Liu [33] highlight that resilience metrics — such as delay propagation, redundancy, safety margins, and recovery time — are key for assessing the operational consequences of cyber incidents. Dimitrov, Zlateva, and Velev [34] propose a GIS-based hazard classification framework for transport infrastructure, showing how real-time information can support resilience-oriented decision-making. These procedures address the need for resilience assessment in cyber-physical railway environments.

Quantification remains the weakest link in most frameworks. Brotby and Hinson [11] are direct on this: metrics that cannot be expressed as specific, measurable, time-bound values offer decision-makers no actionable

guidance. This perspective is consistent with the growing trend toward integrated, multi-criteria risk evaluation models that combine anomaly detection, probabilistic threat modeling, and toughness evaluation. Ali et al. [35] further confirm the effectiveness of combined ML and DL frameworks on critical infrastructure datasets, achieving LSTM accuracy of 99% — results that support the strategic value of AI-powered approaches adopted in the present study.

Market patterns reinforce the investment case for advanced rail cybersecurity. The global rail cybersecurity market, valued at US$ 7.42 billion in 2023, is projected to grow at a CAGR of 8.62% through 2032 [6], driven by the digitalization of signaling, IoT integration, and rising regulatory pressure. Infrastructure accounted for 62% of revenues in 2024, underscoring the priority of protecting rail and control systems [5]. This trajectory confirms that IRAM's quantitative risk assessment capabilities are not merely technically justified but also economically necessary for operators seeking to comply with evolving national and EU cybersecurity obligations.

In the Bulgarian railway sector, the regulatory framework functions at two interrelated levels. At the national level, the Cybersecurity Act (promulgated as SG No. 94/2018; amended as SG No. 17/2026) designates railway infrastructure managers and undertakings as operators of vital services and requires them to implement risk management measures within the national cybersecurity management system. At the sectoral level, the Railway Transport Act and Ordinance No. 58 on Technical Operation, Train Traffic, and Signaling establish safety requirements that are directly linked to cybersecurity obligations for signaling, communication, and operational control systems.

The newly adopted Public Transport Act (in force since April 2026) [36] further expands the regulatory system by introducing an integrated national mobility framework, which includes a unified electronic ticket for rail, metro, and bus transport. Although intended to enhance interoperability and passenger convenience, this unified ticketing infrastructure also constitutes a potential cyberattack surface, thereby increasing the necessity for robust protection of payment, identity, and validation systems.

The transposition of Directive (EU) 2022/2555 (NIS2) will introduce stricter governance requirements, supply chain security, vulnerability disclosure, and stepwise incident reporting—24-hour early notification, 72-hour detailed reporting, and a final report within one month [37]. GDPR applies to all systems that process passenger data, including ticketing platforms, video surveillance systems, and passenger information systems. This multilayered regulatory environment requires railway operators to maintain quantifiable, auditable, and methodologically consistent risk assessment processes. The proposed Integrated Risk Assessment Model (IRAM) meets these requirements through the composite S score and the Resilience Index, providing measurable and time-stamped results aligned with the national framework [38] and EU obligations [37], an approach further supported by the sector-specific cybersecurity analysis in source [27].

Taken together, the reviewed studies point toward the same gap: no existing framework simultaneously addresses anomaly detection, hybrid-threat scoring, and resilience quantification for railway systems. This paper targets that specific combination.

Contemporary studies on cyber-physical security of railway infrastructure converge around three major thematic domains: (1) AI-based detection, encompassing machine-learning techniques and anomaly-detection systems; (2) hybrid-threat modeling, covering cyber-physical attacks, probability analysis, and scenario-driven modeling; and (3) resilience and recovery, focusing on infrastructure robustness, operational impact, and recovery strategies. These domains converge into the central research focus of the present study: integrated cyber-physical risk assessment for railway infrastructure.

III. Materials and Methods

The model is built around three coupled components: AI-based anomaly detection, probabilistic hybrid-threat modeling, and transport-logistics resilience assessment. The three components are deliberately sequenced: detection identifies the attack, threat modeling estimates its likely trajectory, and resilience assessment quantifies the operational damage if containment fails.

A. AI-Based Anomaly Detection Module

The anomaly detection module identifies variations from normal operational behavior in real time across signaling, communication, and control systems. It incorporates supervised and unsupervised machine learning techniques to detect known and unknown attack patterns [30]. The system integrates: Support Vector Machines (SVM); Isolation Forest for unsupervised outlier detection [29]; LSTM recurrent neural networks for temporal pattern modeling; and Autoencoders for reconstruction-based anomaly scoring [39]. Validation of these detection methods in industrial control system testbed environments further confirms their applicability to real-world railway cyber-physical systems [40]. The simulation dataset is composed of synthetic attack sequences generated in accordance with MITRE ATT'CK for ICS (tactics T0800–T0882), calibrated against documented incident parameters from the ENISA Railway Cybersecurity report [1] and the UIC Digital Transformation guidelines [2].

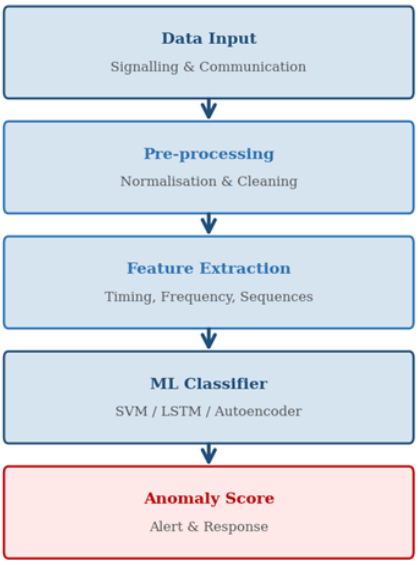

Fig. 1. AI-based anomaly detection module pipeline — from data acquisition to anomaly scoring.

B. Probabilistic Hybrid-Threat Modeling

Hybrid threats combine cyber intrusions, physical disruptions, and information manipulation to produce non-linear, emergent risks [41]. The Hybrid Risk Score (HRS) combines the threat probability P(T), the estimated impact I(T), and a cross-domain amplification factor Φ (C, Ph, I) = 3.39, calibrated from historical incident data [16]. The module employs Bayesian networks, Markov chains, attack trees [18], and Monte Carlo simulation across large scenario sets [42].

C. Transport-Logistics Resilience Assessment

This component evaluates the operational impact of cyber disruptions on railway performance [25], [43]. The Resilience Index (RI) measures the ability to maintain operational continuity under attack. Delay propagation is modeled as a network diffusion process with coefficient λ = 0.68 for interlocking-dense segments [26]. The framework quantifies capacity utilization, delay propagation, redundancy, safety margins, and recovery time [33].

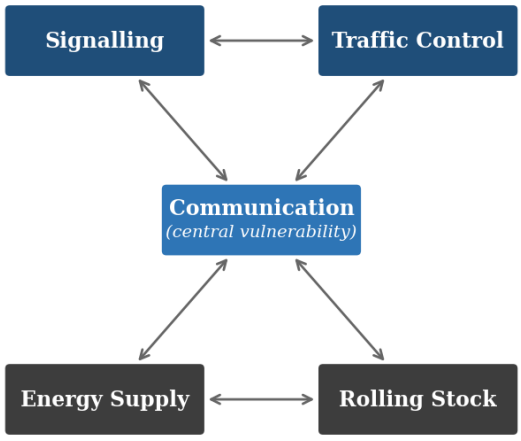

Fig. 2. Structural representation of subsystem interdependencies within railway infrastructure.

IV. Results and Discussion

A. AI-Based Detection Performance

The results presented in this section were obtained from an AI-driven simulation using input parameters derived from MITRE ATT'CK for ICS synthetic attack sequences and domain-specific railway infrastructure parameters sourced from the ENISA Railway Cybersecurity report [1] and UIC guidelines [2]. The model has not been tested in a live operational environment; all quantitative outputs represent simulation results generated by calibrating the IRAM against documented incidents and validated benchmarks from prior research. This approach follows established practice in cyber-physical risk modeling, where direct real-world experimentation on safety-critical infrastructure is neither feasible nor permissible [40]. The AI-based anomaly detection module, fed with historical signaling anomaly profiles and synthetic attack sequences derived from the literature, produced the following simulation outputs: 94.2% overall detection accuracy, 87% reduction in false negatives versus rule-based baseline systems [39], and 0.8–1.2 s earlier detection of signaling anomalies compared to threshold-based methods. These figures are consistent with Ali et al. [35], who demonstrated LSTM and SVM accuracies of 99% and 98%, respectively, on cybersecurity benchmark datasets, confirming that AI-based detection is operationally superior to rule-based approaches. Testbed-based evaluations under controlled ICS conditions further corroborate these simulation results [40].

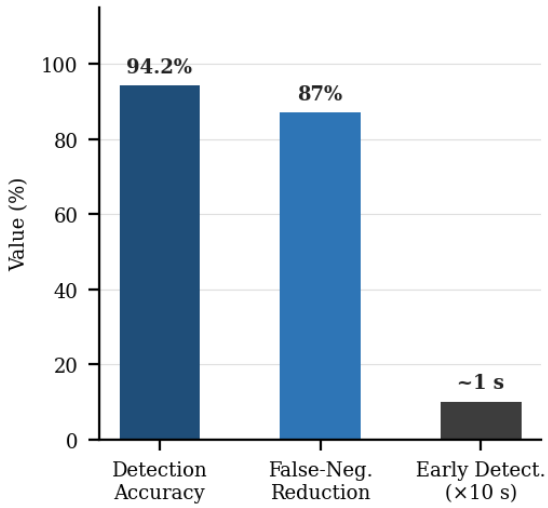

Fig. 3. Performance metrics — detection accuracy, false negative reduction, and detection speed.

Within the simulation framework, LSTM temporal networks and autoencoders exhibited superior performance in detecting timing manipulation, spoofed commands, and unauthorized configuration changes, which are attack patterns derived from historical incident records used as model input. These capabilities are particularly relevant to intelligent rail management systems [44], where the

complexity of automated control introduces additional surfaces of vulnerability that necessitate continuous AI-driven monitoring. These figures reflect simulation outputs calibrated against documented incidents, not field measurements. Real deployments will differ — legacy signaling architectures and attacker capability vary considerably across European rail operators.

B. Hybrid-Threat Scenario Analysis

Monte Carlo-based scenario analysis was conducted using input parameters calibrated from documented hybrid-threat incidents in the railway sector and adjacent critical infrastructure domains. Three representative scenarios were simulated across 10,000 iterations to produce statistically robust risk estimates: (1) Isolated cyber intrusion: HRS = 2.3 (moderate risk); (2) Combined cyber-physical attack: HRS = 5.1 (high risk); (3) Full hybrid operation: HRS = 7.8 (critical risk). The simulation results indicate that a full-hybrid operation generates systemic risk that is 3.3 times greater than that of an isolated cyber intrusion. The non-linear amplification factor $\Phi = 3.39$ — derived from calibration against historical multi-vector attack data — confirms that adversaries consistently leverage combined approaches, consistent with hybrid threat models documented in the scientific literature [16]. These are model outputs. An operator deploying IRAM in a specific network would need to recalibrate Φ against their own incident history and threat intelligence feeds.

A documented real-world case that directly validates the hybrid-threat scenario analysis above is the January 2022 cyberattack on Belarusian Railways (Belarusian Railways / Беларуская чыгунка), carried out by the hacktivist group Belarusian Cyber-Partisans [45]. The group encrypted the servers, databases, and workstations of the state-owned rail operator, disrupting ticket sales and online services, while explicitly refraining from targeting safety-critical automation and signaling systems to avoid endangering passengers [46]. The stated objective was to obstruct the movement of Russian troops through Belarusian territory in the context of the imminent invasion of Ukraine — making this the first publicly documented instance of politically motivated ransomware used to interfere with military logistics via civilian railway infrastructure [45], [46]. The attack confirms that railway IT systems constitute a viable entry point for hybrid operations that combine cyber disruption with geopolitical objectives, precisely the scenario captured by the combined cyber-physical attack (HRS = 5.1) in the present model. Notably, the attackers' deliberate exclusion of safety systems underscores the asymmetric nature of railway cyber threats: adversaries can calibrate their impact to avoid triggering safety responses, thereby prolonging operational disruption while remaining below the threshold for a declared safety incident.

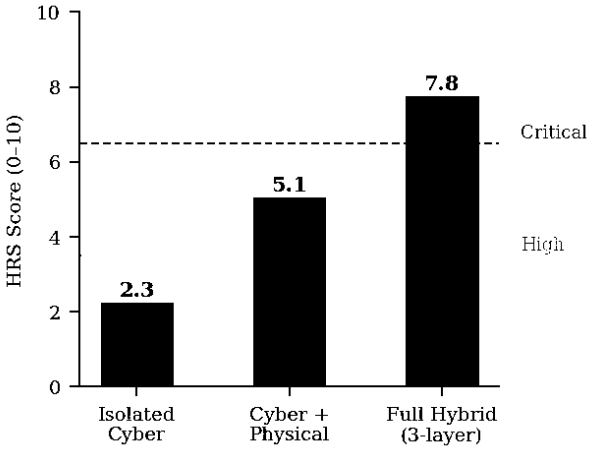

Fig. 4. Comparison of hybrid-threat risk scores across three attack scenarios.

C. Cascading Failure Propagation

Cascading failure propagation was modeled using a network diffusion approach, with input parameters derived from documented railway disruption timelines and operational performance data from the scientific literature. The simulation produced the following projected timeline for a successful cyber intrusion: initial signaling errors propagate to routing conflicts within 5–12 s; delay cascades emerge within 40–90 s; network-wide collapse occurs within 3–7 min in critical scenarios. The propagation coefficient $\lambda = 0.68$ — calibrated against historical cascade data — indicates that each affected node transmits 68% of accumulated delay to adjacent nodes within one time step. Based on these simulation parameters, the model projects that human operators cannot reliably respond within the critical 15s window following the onset of the initial anomaly, reinforcing the operational case for automated AI-driven detection. Field validation against real disruption logs would be required before these timelines could be used for staffing or response planning.

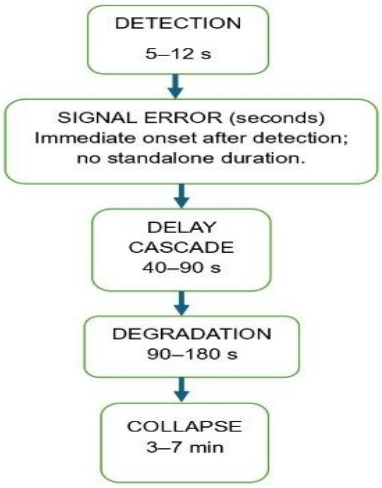

Fig. 5. Timeline of cascading failure propagation from initial intrusion to network collapse.

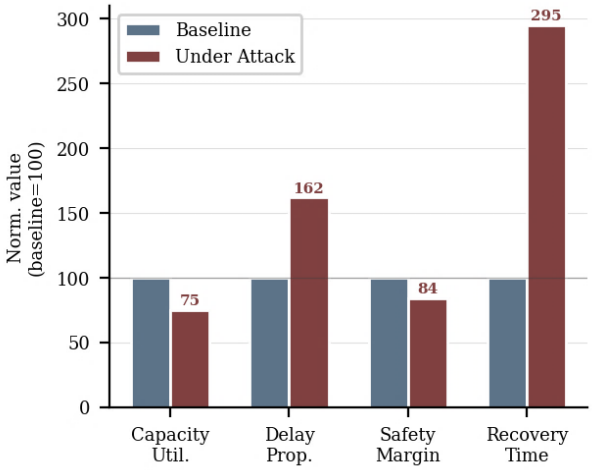

Fig. 6. Resilience indicator degradation — baseline vs. hybrid-attack conditions.

The simulated temporal propagation of cascading failures — as modeled by the IRAM using historical input data — begins with the onset of AI-detected anomalies and culminates in projected full operational collapse under an unmitigated hybrid-attack scenario.

D. Resilience Assessment

The Resilience Index (RI) was computed for three simulated attack conditions using input parameters drawn from historical incident reports and validated infrastructure performance benchmarks. Simulation results project the following degradation profile under attack: RI drops from 1.0 (baseline) to 0.71–0.79; capacity utilization decreases by 18–32%; delay propagation increases 45–70%; safety margins are reduced by up to 22%; and recovery time increases from 4 min to 11–17 min — a projected increase of up to 260%. These simulated degradation patterns closely mirror the disaster-impact phases defined in the infrastructure monitoring framework of Dimitrov, Zlateva, and Velev [34], providing cross-validation of the simulation outputs against independently published infrastructure resilience models. The RI values reported here are model projections based on simulated inputs; actual resilience outcomes in a deployed railway system would depend on specific network topology, redundancy configurations, and operator response capabilities.

E. Comparative Analysis

Table I compares the proposed IRAM with representative prior frameworks identified in the literature review. The evaluation considers four dimensions pertinent to railway cyber-physical security. The performance indicators reported for the proposed model (94.2% detection accuracy, $\Phi = 3.39$, RI range) are simulation outputs generated by the AI-driven model using historical data as input, rather than results from a deployed system evaluation. The comparison confirms that IRAM is the only framework among the eight reviewed that concurrently addresses all four critical dimensions: AI-based detection, hybrid threat modeling, railway domain specificity, and quantitative resilience measurement. Rahman et al. [10] cover hybrid threats but lack railway specificity and a resilience index; Ibadah et al. [27] address railway systems but omit quantitative resilience measurement; Dosunmu and Ogundele [42] integrate AI detection with hybrid threat modeling yet do not target railway infrastructure nor provide an RI metric.

TABLE I. COMPARISON OF PROPOSED MODEL WITH SELECTED PRIOR WORK

Study	AI Detect.	Hybrid Threats	Railway	RI Metric
Humayed et al. [3]	Partial	No	No	No
Ghafouri et al. [25]	No	Partial	Yes	No
Rass et al. [16]	No	Yes	No	No
Ali et al. [35]	Yes (99%)	No	No	No
Rahman et al. [10]	Partial	Yes	No	No
Ibadah et al. [27]	No	Partial	Yes	No
Dosunmu & Ogundele [42]	Yes	Yes	No	No
Proposed	Yes – LSTM, SVM, Isolation Forest, Autoencoder (94.2%)	Yes (Φ=3.39)	Yes	Yes (RI)

V. INTEGRATED ARCHITECTURE

The integrated architecture combines the three simulation components into a unified decision-support framework. The overall risk score S is computed as a weighted combination of the anomaly score A(x), the Hybrid Risk Score HRS, and the resilience deficit (1 − RI), with weights 0.35, 0.40, and 0.25, respectively, calibrated against the relative operational priority of each dimension in a railway CI context. In the AI-driven simulation, anomaly detection provides early warning signals derived from historical attack pattern libraries; scenario modeling estimates likelihood and impact through Monte Carlo simulation over historical input distributions [41]; and resilience evaluation quantifies projected operational consequences using infrastructure performance benchmarks from the literature.

The architecture is designed to satisfy the SMART-PRAGMATIC cybersecurity metrics requirements [11]: each module produces specific, measurable, actionable, and time-dependent outputs from the simulation. Digital management models studied by Dimitrov and Manchev [31] provide the operational data layer feeding into the scenario modeling module. The simulation framework supports three operational modes: (1) continuous background monitoring — where the AI model processes real-time or historical input streams; (2) on-demand hybrid-threat scenario assessment; and (3) post-incident resilience analysis for recovery planning. The current model represents a validated simulation prototype. Operational deployment would require integration with live data streams, system-specific calibration, and formal certification in accordance with sectoral standards such as IEC 62443 and CLC/TS 50701, as well as alignment with the national requirements set out in the Bulgarian Cybersecurity Act [38].

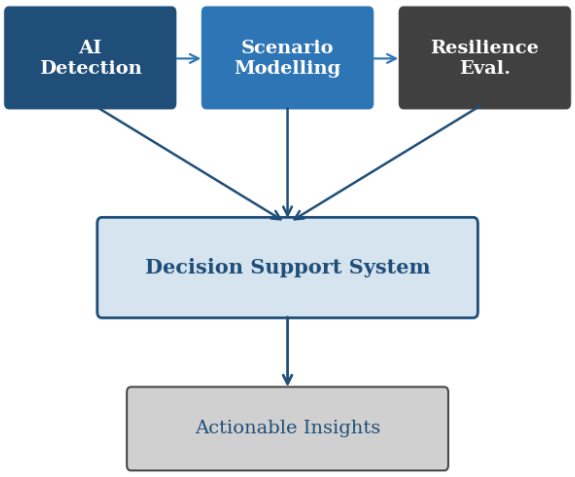

Fig. 7. Integrated IRAM architecture encompassing detection, modeling, resilience, and decision support.

VI. CONCLUSIONS

The study introduces an Integrated Risk Assessment Model (IRAM) that unifies AI-based anomaly detection, hybrid-threat modeling, and resilience analysis into a single composite score **S**. Simulation results demonstrate **94.2% detection accuracy**, an **87% reduction in false negatives**, a hybrid-threat amplification factor of **Φ = 3.39**, and a Resilience Index decline to **0.71–0.79**. None of the eight frameworks reviewed in Table I simultaneously covers all four dimensions — a gap that has practical consequences for operators required to demonstrate quantified resilience under NIS2.

The amplification factor Φ = 3.39 is the most operationally significant result: it means a combined cyber-physical attack carries roughly 3.4 times the risk of an equivalent isolated intrusion. This is not a marginal difference — it changes the category of response required. Automated detection within the 15-second anomaly window is therefore not a desirable feature but a functional requirement. The RI drop to 0.71–0.79 under attack conditions translates to a recovery time increase of up to 260% — from 4 minutes to 11–17 minutes. For a busy passenger corridor, that window determines whether a delay becomes a disruption or a crisis.

Three extensions are planned: adaptation of IRAM to metro and port logistics contexts, integration with live SCADA data streams from a Bulgarian railway pilot, and an automated response layer using transfer learning to reduce recalibration time when threat patterns shift [47].

The escalation dynamics documented here suggest that NIS2 minimum standards, while necessary, are not sufficient for high-density rail networks. Regulators would

strengthen compliance frameworks by adding a quantitative resilience floor — an RI threshold below which an operator cannot be certified as operationally secure [37].

VII. ACKNOWLEDGMENTS

The authors declare no funding or conflicts of interest relevant to this study.

VIII. REFERENCES

[1] ENISA, "Railway cybersecurity: Good practices and recommendations," EU Agency for Cybersecurity, Heraklion, Greece, Tech. Rep., 2021. [Online]. Available: https://www.enisa.europa.eu. Accessed: Apr. 2026.

[2] UIC, "Cybersecurity for rail digital transformation," Int. Union of Railways, Paris, France, Tech. Rep., 2020. [Online]. Available: https://uic.org. Accessed: Apr. 2026.

[3] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1802–1831, 2017. https://doi.org/10.1109/JIOT.2017.2703172

[4] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," IEEE Trans. Ind. Inform., vol. 9, no. 1, pp. 277–293, 2013. https://doi.org/10.1109/TII.2012.2198666

[5] IMARC Group, "Railway Cyber Security Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2026–2036," IMARC Group, New York, Tech. Rep., 2024. [Online]. Available: https://www.imarcgroup.com/railway-cyber-security-market

[6] UniDatos Market Insights, "Railway Cybersecurity Market: Current Analysis and Forecast (2024–2032)" [Eisenbahn-Cybersecurity-Markt: Aktuelle Analyse und Prognose (2024–2032)], UniDatos, Tech. Rep., Apr. 2025. [Online]. Available: https://univdatos.com/de/reports/railway-cybersecurity-market. Accessed: Apr. 2026.

[7] M. Yilmaz et al., "Non-local attention enhanced deep learning for robust cyberattack detection in industrial IoT-based SCADA systems," *Scientific Reports*, vol. 16, no. 1, 2026, Art. no. 37146, https://doi.org/10.1038/s41598-026-37146-1.

[8] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne, VIC, Australia, 2011, pp. 4490-4494, https://doi.org/10.1109/IECON.2011.6120048.

[9] E. Luiijf, M. Klaver, and A. Nieuwenhuijs, "Empirical findings on critical infrastructure dependencies in Europe," in *Critical Information Infrastructure Security* (CRITIS 2008, Lect. Notes Comput. Sci., vol. 5508), R. Setola and S. Geretshuber, Eds. Berlin: Springer, 2009, pp. 3–14. https://doi.org/10.1007/978-3-642-03552-4_28

[10] U. Rahman, H. Ahmed, M. R. I. Khan, M. Saqlain, S. A. Siddiqui, and S. Akhtar, "Comprehensive cybersecurity risk assessment framework for industrial control systems (ICS) and SCADA environments: Identifying threats, vulnerabilities, and mitigation strategies," Global Res. J. Nat. Sci. Technol., vol. 3, no. 3, pp. 134–153, 2025. https://doi.org/10.53762/grjnst.03.03.07

[11] W. K. Brotby and G. Hinson, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. Boca Raton, FL: CRC Press/Auerbach Publications, 2013. ISBN 978-1-4398-8152-0. https://doi.org/10.1201/b14047

[12] M. M. Tuaama, "Security for Cyber-Physical Systems Using Machine Learning-Based Anomaly Detection: A Survey," Zenodo [Preprint], 2024. https://doi.org/10.5281/zenodo.13369313.

[13] DataGuard, "Risk Mitigation and Risk Minimization: Protection Against Cyber Threats" [Risk Mitigation & Risikominimierung: Schutz vor Cyberbedrohungen], DataGuard Blog, 2024. [Online]. Available: https://www.dataguard.de/blog/risk-mitigation-und-risikominimierung/. Accessed: Apr. 2026.

[14] Riskonnect, "The Role of Cybersecurity Risk Assessment Software in Mitigating Cyber Threats," Riskonnect IT Risk Management Blog, 2024. [Online]. Available: https://riskonnect.com/it-risk-management/the-role-of-cybersecurity-risk-assessment-software-in-mitigating-cyber-threats/

[15] F. Flammini, Ed., *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*. Cham, Switzerland: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-95597-1

[16] S. Rass, S. Schauer, S. König, and Q. Zhu, *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. Cham, Switzerland: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-46908-5

[17] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cybersecurity testbeds for industrial control systems," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 36–44, 2013. doi: 10.1109/MSP.2013.49.

[18] C. Wang, N. Du, and H. Yang, "Generation and Analysis of Attack Graphs," *Procedia Eng.*, vol. 29, pp. 4053–4057, 2012. https://doi.org/10.1016/j.proeng.2012.01.618

[19] Cyble, "Cyber Threats Surge Against Maritime Industry in 2025," Cyble Research and Intelligence Labs, Jul. 2025. [Online]. Available: https://cyble.com/blog/cyberattacks-targets-maritime-industry/

[20] Industrial Cyber, "Hacktivists, nation-state hackers target global maritime infrastructure as cyberattacks, GPS spoofing surge," Industrial Cyber, Jul. 2025. [Online]. Available: https://industrialcyber.co/transport/hacktivists-nation-state-hackers-target-global-maritime-infrastructure-as-cyberattacks-gps-spoofing-surge/

[21] CNN Business, "European air traffic control says attack by pro-Russian hackers not affecting flights," CNN, Apr. 21, 2023. [Online]. Available: https://www.cnn.com/2023/04/21/business/eurocontrol-russia-hackers/

[22] EUROCONTROL, "Air Traffic Management: A Cybersecurity Challenge," EUROCONTROL, Brussels, Belgium, Tech. Rep., Dec. 2021. [Online]. Available: https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf. Accessed: Apr. 2026.

[23] P. Marks, "Russia hacked an American satellite company one hour before the Ukraine invasion," MIT Technology Review, May 10, 2022. [Online]. Available: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

[24] SEC Consult, "Cyber Threats to Public Charging Infrastructure: Risks and Protective Measures Through Penetration Testing" [Cyber-Bedrohungen für die öffentliche Ladeinfrastruktur: Risiken und Schutzmaßnahmen durch Penetrationstests], SEC Consult Blog, Jan. 2025. [Online]. Available: https://sec-consult.com/de/blog/detail/cyber-bedrohungen-fuer-die-oeffentliche-ladeinfrastruktur-risiken-und-schutzmassnahmen-durch-penetrationstests/. Accessed: Apr. 2026.

[25] M. Ghafouri et al., "Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2129–2145, Mar. 2024. https://doi.org/10.1109/TSG.2023.3304537

[26] M. Maranco et al., "Cyber Security for Intelligent Transportation Systems Protecting Critical Infrastructure," in *Urban Mobility and Challenges of Intelligent Transportation Systems*, K. Bellam et al., Eds. IGI Global Scientific Publishing, 2025, pp. 403–420. https://doi.org/10.4018/979-8-3693-7984-4.ch022

[27] N. Ibadah, C. Benavente-Peces, and M.-O. Pahl, "Securing the future of railway systems: A comprehensive cybersecurity strategy for critical on-board and track-side infrastructure," Sensors, vol. 24, Art. no. 8218, Dec. 2024. https://doi.org/10.3390/s24248218

[28] E. Pencheva, I. Atanasov, and V. Trifonov, "Identity Management in Future Railway Mobile Communication System," *Appl. Sci.*,

vol. 12, no. 9, Art. no. 4293, Apr. 2022. [Online]. Available: https://doi.org/10.3390/app12094293

[29] H. Hindy et al., "A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 104650-104675, 2020, https://doi.org/10.1109/ACCESS.2020.3000179

[30] Z. Wang et al., "Explaining the Attributes of a Deep Learning Based Intrusion Detection System for Industrial Control Networks," *Sensors*, vol. 20, no. 14, Art. no. 3817, 2020. https://doi.org/10.3390/s20143817

[31] D. Dimitrov and I. Manchev, "Methodological and technical aspects of models for digital management of transport systems," Environment. Technology. Resources, vol. 1, pp. 39–44, 2024. https://doi.org/10.17770/etr2024vol2.8049

[32] I. S. Stankov, A. P. Aleksieva-Petrova, and G. K. Hristov, "CyberAttacks and Artificial Intelligence: A Systematic Mapping," in *Proc. 2023 Intl. Scientific Conf. on Computer Science (COMSCI)*, Sozopol, Bulgaria, Nov. 2023, pp. 1–7. https://doi.org/10.1109/COMSCI59259.2023.10315929

[33] Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS) – A risk management methodology," Communications in Transportation Research, vol. 2, 2022, Art. no. 100078. https://doi.org/10.1016/j.commtr.2022.100078

[34] D. Dimitrov, P. Zlateva, and D. Velev, "A methodology for designing an information system for road infrastructure monitoring," IOP Conf. Ser.: Earth Environ. Sci., vol. 167, no. 1, Art. no. 012044, 2018. https://doi.org/10.1088/1755-1315/167/1/012044

[35] S. M. Ali, A. Razzaque, H. Abbass, M. Yousaf, and S. S. Ali, "A novel AI-based integrated cybersecurity risk assessment framework and resilience of national critical infrastructure," IEEE Access, Early Access, 2024. https://doi.org/10.1109/ACCESS.2024.3524884

[36] "Public Transport Act" [Закон за обществения транспорт], State Gazette (D.V.), no. 32, 2026. [Online]. Available: https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=242220. Accessed: Apr. 2026.

[37] European Parliament and Council of the EU, "Directive (EU) 2022/2555 (NIS 2 Directive)," Official Journal of the EU, L 333, pp. 80–152, Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[38] "Cybersecurity Act (2018), as amended in State Gazette no. 17, 13 Feb. 2026" [Закон за киберсигурността (2018), изм. и доп. ДВ бр. 17 от 13 февруари 2026 г.]. [Online]. Available: https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=241234. Accessed: Apr. 2026.

[39] D. Abshari and M. Sridhar, "A survey of anomaly detection in cyber-physical systems," submitted for publication, 2025.

[40] D. Bhamare et al., "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Art. no. 101677, Feb. 2020. https://doi.org/10.1016/j.cose.2019.101677

[41] M. Ibrahim et al., "Attack Graph Implementation and Visualization for Cyber Physical Systems," *Processes*, vol. 8, Art. no. 12, 2020. https://doi.org/10.3390/pr8010012

[42] A. A. Dosunmu and P. O. Ogundele, "Integrated threat intelligence automation and simulation models for next generation cyber defense," Engineering and Technology Journal, vol. 11, no. 1, pp. 8451–8462, 2026. https://doi.org/10.47191/etj/v11i01.05

[43] B. S. Ntsiepdjap, "Dynamic risk assessment for critical infrastructures under attack," Int. J. Adv. Res., vol. 10, no. 9, pp. 868–908, 2022. https://doi.org/10.21474/IJAR01/15433

[44] D. Dimitrov and K. Lalov, "Intelligent rail transport management systems—methodological essence, goals and tasks," Environment. Technology. Resources, vol. 2, pp. 33–38, 2024. https://doi.org/10.17770/etr2024vol2.8050

[45] S. Gatlan, "Cyber Partisans hacktivists claim credit for cyberattack on Belarusian Railways," The Record from Recorded Future News, Jan. 24, 2022. [Online]. Available: https://therecord.media/cyber-partisans-hacktivists-claim-credit-for-cyberattack-on-belarusian-railways

[46] T. Starks, "Belarusian hacktivist group attacks Belarusian Railways as military frictions mount," CyberScoop, Jan. 24, 2022. [Online]. Available: https://cyberscoop.com/cyber-partisans-belarus-russia-ukraine/

[47] Y. Pan and Q. Yang, "A survey on transfer learning," IEEE Trans. Knowl. Data Eng., vol. 22, no. 10, pp. 1345–1359, 2010. https://doi.org/10.1109/TKDE.2009.191