



GCCR

Global Conference on
Contemporary Research

INTERNATIONAL CONFERENCE ON LANGUAGES, LITERATURE AND CULTURAL STUDIES

CONFERENCE THEME:

Language, Culture and Innovation:
Bridging Global Perspectives
through Research.



LANGUAGE
STUDIES



LITERATURE



CULTURAL
STUDIES



INTERNATIONAL
COLLABORATION

INTERNATIONAL CONFERENCE
PEER-REVIEWED PROCEEDINGS



OCTOBER
2026



NEW YORK, USA



gccr.academy



GCCR

INTERNATIONAL CONFERENCE ON
LANGUAGES, LITERATURE AND CULTURAL STUDIES

OCTOBER 2026

NEW YORK, USA





THE ROLE OF DIGITAL TECHNOLOGIES IN ENSURING RAILWAY TRANSPORT SAFETY

Ibragimova Gulshan Ruslanovna

PhD, Associate Professor,

Department of Railway Operation Management,

Tashkent State Transport University, Tashkent, Uzbekistan.

Abduvaitova Maria Temur qizi

Master's Student, Department of Railway Operation Management,

Tashkent State Transport University, Tashkent, Uzbekistan.

<https://doi.org/10.5281/zenodo.23284249>

Abstract. The rapid integration of digital technologies—encompassing Artificial Intelligence (AI), Digital Twins (DT), and the Internet of Things (IoT)—is fundamentally transforming railway transport safety. This paper presents a critical scientific literature review of recent peer-reviewed advancements in digital railway safety systems, evaluating their operational efficacy, implementation challenges, and theoretical boundaries. The review synthesizes findings on AI-driven predictive maintenance, which transitions railways from reactive troubleshooting to continuous condition-based monitoring, alongside the use of Digital Twins for risk-free virtual simulations. Furthermore, the convergence of Information Technology (IT) and Operational Technology (OT) in intelligent signalling systems, such as the European Rail Traffic Management System (ERTMS), is examined through the lens of emerging cybersecurity vulnerabilities. Despite significant technological maturation, a critical research gap persists regarding the formal regulatory certification of probabilistic machine learning algorithms for high Safety Integrity Level (SIL) applications. The study concludes that while digital technologies dramatically enhance anomaly detection and system resilience, their integration into autonomous, safety-critical environments relies heavily on the future development of Explainable AI (XAI) validation frameworks and holistic IT-OT cybersecurity models.

Keywords: Railway Safety, Artificial Intelligence, Digital Twins, Predictive



Maintenance, Cybersecurity, Intelligent Transportation Systems.

Introduction. Historically, railway transport safety has relied on fail-safe electro-mechanical principles, redundant circuitry, and highly structured, interval-based maintenance schedules. However, the modernization of railway networks and the demand for increased capacity have necessitated a shift toward continuous, data-driven safety assurance. Today, the modern railway network operates as an interconnected Cyber-Physical System (CPS), wherein physical infrastructure, rolling stock, and signalling components are continuously monitored and controlled by complex digital architectures [1].

The primary objective of implementing digital technologies in rail transport is to minimize human error, optimize infrastructure resilience, and transition operations from reactive emergency troubleshooting to proactive predictive maintenance [2]. Recent technological advancements in distributed sensor networks, edge computing, and machine learning have unlocked unprecedented capabilities for real-time risk assessment and structural health monitoring. Nevertheless, the digitization of railway operations introduces a paradox: as systems become more autonomous and interconnected, their operational complexity and vulnerability to cyber threats scale exponentially [1], [5]. This manuscript critically evaluates the contemporary scientific literature concerning the application of digital technologies in railway transport safety. By critically comparing verified, peer-reviewed research, this review identifies critical gaps between algorithmic innovation and deterministic regulatory certification, highlighting the conditions and limitations of integrating digital tools into life-critical transport systems.

Literature Review and Critical Analysis

Artificial Intelligence and Predictive Maintenance. Artificial Intelligence and Machine Learning (ML) have established a dominant presence in recent railway safety research. In a foundational literature review, Tang et al. [2] established that AI applications effectively transition railway operations from periodic, interval-based checks to condition-based interventions. By analyzing vast quantities of historical and real-time



operational data, AI models can identify subtle patterns of wear and degradation that traditional mathematical models often overlook, thereby maximizing both track lifespan and passenger safety [2].

Recent empirical research reinforces the transition toward AI-driven infrastructure management. Šmajda and Kendra [4] investigated the use of Artificial Intelligence for the predictive maintenance of railway infrastructure, emphasizing how machine learning algorithms leverage continuous telemetry to anticipate faults before they compromise operational safety. By deploying AI, infrastructure managers can dynamically optimize maintenance schedules, reducing unnecessary manual inspections and limiting the probability of unexpected track defects [4].

Despite these empirical successes in operational optimization, the scientific literature identifies a significant regulatory barrier preventing the use of AI in autonomous railway safety control. The European standard EN 50716:2023 (which unifies and supersedes the widely cited EN 50128 and EN 50657 standards) governs software development for railway applications. While this standard does not explicitly prohibit AI, it mandates rigorous traceability, complete test coverage, and mathematically verifiable, deterministic logic for software assigned to Safety Integrity Level 3 (SIL 3) and SIL 4. Because deep neural networks derive their decision boundaries probabilistically from training data rather than via programmed logical operators, formal verification of their behavior under unforeseen edge cases remains an unresolved engineering challenge. Consequently, current AI applications in rail are largely recommended for non-SIL advisory and monitoring tasks, rather than autonomous, life-critical decision-making operations such as electronic interlocking or automatic train protection [4], [7].

Digital Twins and Sensor-based Monitoring. To safely validate predictive models and optimize physical interventions without jeopardizing live railway assets, researchers have increasingly turned to Digital Twin (DT) technology. A comprehensive survey by Ghaboura et al. [3] defines a railway Digital Twin not merely as a static 3D geometric model, but as a dynamic virtual replica continuously updated via Internet of Things (IoT)



sensor telemetry. Digital Twins serve as risk-free computational environments where complex failure scenarios can be simulated, and the health of the railway cyber-physical system can be monitored continuously [3].

Sensor-based monitoring is the foundational data source that feeds these digital models. A practical demonstration of this is provided by Stypułkowski et al. [6], who researched the safety benefits of continuous Structural Health Monitoring (SHM) by applying thermal imaging analysis to the electric heating of turnouts. Turnouts and switches are highly vulnerable to freezing during severe winter conditions, posing severe derailment risks. Their research indicates that automated thermographic analysis can accurately detect heating anomalies in real-time, preventing switch failures [6]. Such sensor data, when integrated into a broader Digital Twin framework, allows infrastructure managers to achieve a holistic view of network health [3].

However, the primary limitation identified across the DT and SHM literature is data interoperability and signal noise. Real-world railway environments generate unstructured data with inconsistent sampling rates and severe environmental interference. Consequently, before data can be reliably utilized for safety assessments, advanced data-fusion and preprocessing frameworks must be implemented to filter environmental noise, representing a significant engineering challenge that must be addressed before digital twins can fully replicate physical reality [3], [4].

Cybersecurity in Intelligent Signalling Systems. The deployment of Intelligent Transportation Systems (ITS) and radio-based signalling architectures, such as the European Rail Traffic Management System (ERTMS), represents a critical shift in railway safety operations. By transitioning from trackside optical signals to continuous wireless communication networks, trains operate with dynamic movement authorities, vastly improving network capacity and reducing the margins for human error [5].

However, this technological transition dissolves the traditional isolation between Information Technology (IT) and Operational Technology (OT). Soderi, Masti, and Zacchia Lun [5] emphasize that modern railways are now highly susceptible to cyber-



attacks that directly impact physical safety. In an interconnected ERTMS environment, a compromised communication link is not merely a data breach; it is a life-threatening hazard. Cyber vulnerabilities could theoretically lead to unauthorized route settings, denial-of-service attacks against control centers, or the malicious suppression of emergency braking commands [5].

Zgorzelski et al. [1] argue that digital integration requires a holistic, multi-level cybersecurity protection system that treats cyber threats as equivalent to physical safety hazards. To safely evaluate these risks, researchers advocate for the use of "cyber ranges"—virtualized network emulations that allow engineers to test railway signalling vulnerabilities against rigorous standards, such as ISA/IEC 62443, without disrupting live commercial traffic [5].

The urgency of this integration is heavily reflected in regulatory trends. A 2026 industry report by the Cyber Senate [7] highlights the impact of European legislative mandates [1]. Specifically, the NIS2 Directive (Directive (EU) 2022/2555) officially designates rail transport as a sector of high criticality, imposing strict statutory cybersecurity risk-management and incident-reporting obligations. Consequently, European railway operators are increasingly required to integrate these cyber-risk frameworks directly into the statutory Safety Management Systems (SMS) governed by the Railway Safety Directive (EU 2016/798). The literature and industry consensus collectively affirm that in the digital era, physical railway safety is inextricably linked to cryptographic security and network resilience [1], [5], [7].

Research Gaps and Discussion. A critical comparison of the reviewed literature reveals a pronounced dichotomy in modern railway digitization: established findings demonstrate that the technological capacity to process data and predict mechanical failures has rapidly matured, yet this innovation substantially outpaces the regulatory frameworks required to certify these systems for autonomous operation.

The principal research gap identified in the literature is the lack of standardized Explainable AI (XAI) validation methodologies tailored to high-tier railway safety



standards. While predictive machine learning models exhibit high empirical success in condition-based maintenance (as demonstrated by Tang et al. [2] and Šmajda and Kendra [4]), their probabilistic architecture restricts them from being certified for life-critical SIL 3 or SIL 4 applications. Future research must prioritize engineering domain-specific XAI frameworks that can mathematically translate complex neural network outputs into the deterministic, transparent safety evidence required by regulatory auditors. Until the logic of AI can be formally verified against strict standard parameters, its role will likely remain confined to advisory and secondary monitoring functions. Additionally, future studies must develop unified metrics that simultaneously evaluate both the physical safety and the cyber-resilience of interconnected railway networks, bridging the remaining divide between IT and OT engineering.

Conclusion. Digital technologies have irrevocably redefined the paradigms of railway transport safety. Artificial Intelligence, IoT-enabled Structural Health Monitoring, and Digital Twins provide infrastructure managers with the unprecedented ability to detect infrastructural anomalies proactively, significantly reducing the reliance on reactive maintenance. Furthermore, intelligent signalling systems have drastically minimized the margins for human error. However, transforming the railway into an interconnected cyber-physical system introduces severe cybersecurity vulnerabilities that require continuous, standards-compliant mitigation. For digital technologies to assume direct control over life-critical operations in the future, subsequent academic and industrial research must bridge the gap between probabilistic machine learning capabilities and deterministic safety certification through the advancement of Explainable AI and robust IT-OT cybersecurity frameworks.

REFERENCES

1. R. Zgorzelski, J. Murawski, and N. Chamier-Gliszczyński, "Digital technologies and cybersecurity of transport infrastructure: challenges for rail transport," *Archives of Transport*, vol. 75, no. 3, pp. 141–158, 2025. DOI: 10.61089/aot2025.yfgz9c91.



2. R. Tang, L. De Donato, N. Bešinović, F. Flammini, R. M. P. Goverde, Z. Lin, R. Liu, T. Tang, V. Vittorini, and Z. Wang, "A literature review of Artificial Intelligence applications in railway systems," *Transportation Research Part C: Emerging Technologies*, vol. 140, Art. no. 103679, 2022. DOI: 10.1016/j.trc.2022.103679.
3. S. Ghaboura, R. Ferdousi, F. Laamarti, C. Yang, and A. El Saddik, "Digital Twin for Railway: A Comprehensive Survey," *IEEE Access*, vol. 11, pp. 120237–120257, 2023. DOI: 10.1109/ACCESS.2023.3327042.
4. M. Šmajda and M. Kendra, "Predictive Maintenance of Railway Infrastructure Using Artificial Intelligence," *Transport Technic and Technology*, vol. 22, no. 1, pp. 1–6, 2026. DOI: 10.2478/ttt-2026-0001.
5. S. Soderi, D. Masti, and Y. Zacchia Lun, "Railway Cyber-Security in the Era of Interconnected Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 6764–6779, 2023. DOI: 10.1109/TITS.2023.3254442.
6. K. Stypułkowski, P. Gołda, K. Lewczuk, and J. Tomaszewska, "Monitoring System for Railway Infrastructure Elements Based on Thermal Imaging Analysis," *Sensors*, vol. 21, no. 11, Art. no. 3819, 2021. DOI: 10.3390/s21113819.
7. Cyber Senate, "Rail Cybersecurity: Key UK, European and North American Developments," Industry Report, Sep. 2026. [Online]. Available: <https://cybersenate.com/rail-cybersecurity-developments/>

