THE BALTIC JOURNAL
OF ROAD AND BRIDGE ENGINEERING
2026/21(3)

ISSN 1822-427X/eISSN 1822-4288
2026 Volume 21 Issue 3: 103–119
https://doi.org/10.7250/bjrbe.2026-21.684

A PREPAREDNESS INDEX FOR CROSS-BORDER RAILWAY LOGISTICS CORRIDORS: INTEGRATING SITUATIONAL AWARENESS, CYBERSECURITY, AND COMMUNICATION REDUNDANCY

ALDONA JARAŠŪNIENĖ*, MARIUS GELŽINIS, DARIUS BAZARAS

Department of Logistics and Transport Management, Vilnius Gediminas Technical University, Vilnius, Lithuania

Received 07 May 2026; accepted 28 August 2026

Abstract. Technologically advanced defence infrastructure and railway information systems are achieving high levels of interoperability by creating a converged architecture that integrates airborne surveillance platforms, command-and-control networking principles, endpoint cybersecurity, and satellite communications. This paper proposes a consolidated approach that combines situational awareness principles (AWACS), a redundant satellite communications channel (Starlink) for telemetry and traffic coordination, and the implementation of proven security practices used in macOS (Secure Enclave, System Integrity Protection, Sandboxing, Gatekeeper, XProtect, Transparency, Consent & Control) in the landscape of railway information systems (SCADA, ERTMS, FRMCS). The methodological basis was modelling and simulation in MATLAB (System Composer, Requirements Toolbox), with control over the fulfilment of requirements for the EN 50126/50128/50129 standards and fault-tolerance assessment through scenarios of communication failures and cyber-attacks. The efficiency assessment is based on the KPIs of availability, delay, packet loss, fault tolerance, and recovery time, as well as the interoperability criteria enshrined in TAF/TAP

* Corresponding author. E-mail: aldona.jarasuniene@vilniustech.lt

Aldona JARAŠŪNIENĖ (ORCID ID 0000-0002-9804-0064)
Marius GELŽINIS (ORCID ID 0009-0000-4786-9297)
Darius BAZARAS (ORCID ID 0000-0002-0603-7678)

TSI, RINF, and eFTI. The results suggest that architectures with multi-layered monitoring and a strict trust policy for software components enhance the resilience and manageability of corridors against communication failures and targeted cyber-attacks.

Keywords: AWACS, cross-border corridor, digital security, hardware security modules, interoperability, macOS, rail system, resilience, Starlink.

Introduction

The railway system is a complex infrastructure that is both critical and vulnerable to national and interstate security. This is particularly relevant to cross-border railway corridors operating amid geopolitical instability and hybrid threats. First, this is relevant for countries that are at the junction of military-political blocs or directly involved in the war – the countries of the eastern flank of the EU, NATO, and Ukraine. In fact, under such conditions, cross-border railway corridors serve as strategic channels for transporting goods, requiring measures to ensure protection and operational compatibility. Ensuring the uninterrupted operation of these corridors has therefore become a strategic priority. The following barriers limit the scope of research issues of digital security of railway corridors:

- Multi-domain threats to information (corporate systems, API), operational (SCADA, ERTMS) technologies, as well as radio systems (GSM-R, FRMCS);
- Suppression of communication and navigation channels;
- Heterogeneity of standards and the maturity of participants' digital systems;
- Insufficient real-time monitoring in cross-border operations.

Since the beginning of the Russian Federation's full-scale war against Ukraine, the implementation of import-export operations via the Black Sea has become problematic, thereby increasing the burden on land logistics chains and border crossings. As a response, the Solidarity Routes initiative was introduced to support alternative logistics corridors. According to the European Commission's report on this program, railways account for 50% of Ukraine's export volumes to the EU, despite the blockade of maritime logistics routes. The document also emphasises the importance of their functioning in emergencies, as well as the need for digitalisation and security. Without improving these components, the system is vulnerable to failures and attacks (EU-Ukraine Solidarity Lanes, n.d.). This thesis is also supported by articles from the Associated Press and the Wall Street Journal reporting cyberattacks in 2022–2023 targeting logistics hubs, particularly railway information systems. As a result of these attacks, the US and NATO classified these actions as part of a hybrid war that aimed to paralyse key supply chains (Klepper, 2025). Bonin (2025) also points out that railway corridors between the EU and Ukraine need to implement protective mechanisms for the digital environment of rail transport, thereby enabling the formation of a logistics

core in the zone of potential military intervention. NATO, in its "Cyber Defence & Transport Infrastructure" strategy, highlights the crucial importance of transport for the sustainable functioning of allied forces and advises applying the principles of situational awareness (AWACS) and developing a distributed surveillance architecture within transport systems (NATO, 2026).

Within the evolving discourse on resilience and crisis management, preparedness is increasingly recognised as a critical component of system resilience. This signifies a shift from mainly response-focused frameworks towards proactive governance strategies for risk mitigation (Nickdoost et al., 2024). The use of composite indices, such as the Global Health Security Index, the Climate Readiness Index, and the Logistics Performance Index, demonstrates a growing reliance on multidimensional indicators that enable the assessment of complex systems in a way that is comparable, measurable, and practically applicable (Nickdoost et al., 2024). However, despite this progress, the transportation sector lacks integrated, quantitative frameworks that simultaneously capture technological, organisational, and operational preparedness. This gap is especially significant with respect to hybrid threats, which include cyberattacks, communication failures, and geopolitical instability that directly threaten the continuity of supply chains and mobility networks (Kharrat et al., 2025). Therefore, improving conceptual frameworks and practical tools for evaluating transportation preparedness is a strategic necessity.

To address this limitation, recent research has introduced composite index frameworks that consolidate multiple dimensions into a unified metric. One prominent example is the Resilience Index (RI), developed to quantitatively assess and monitor the resilience of road transportation systems to hazards such as flooding and storms (Nickdoost et al., 2024). While RI frameworks represent a significant step forward, they remain primarily tailored to climate-related or physical-hazard contexts, with limited attention to crisis preparedness in logistics and transport operations amid hybrid threats.

Building on this conceptual foundation, this study proposes a Preparedness Index (PI) specifically designed for cross-border railway systems operating under hybrid-threat conditions. The proposed framework extends the logic of composite resilience indicators by integrating three complementary dimensions: technological preparedness (availability, delay, packet loss, recovery time, interoperability metrics), organisational preparedness (institutional coordination mechanisms and maturity of Standard Operating Procedures), and operational preparedness (training frequency, response times, and staff readiness).

The PI therefore provides not only a quantitative assessment framework but also a management-oriented decision-support tool that links technical system performance to governance, coordination, and operational continuity requirements in cross-border railway corridors.

1. Literature review

In this research article, the stability of a cross-border railway corridor is defined as the ability of a railway line to maintain the coordination, integrity, and legal significance of digital and operational processes in the event of segment failures, malicious cyber actions, and communication degradation. In this context, corridor resilience is not limited to the physical robustness of infrastructure; it also depends on the capacity of digital systems to maintain situational awareness, ensure trusted coordination, and sustain continuity of communications under disrupted conditions. Accordingly, the theoretical basis of this study is built on three complementary principles: AWACS-inspired situational awareness, LEO-based communication redundancy, and secure-by-design software trust mechanisms adapted from macOS for railway information systems.

The first conceptual pillar is situational awareness based on AWACS principles. According to the US Air Force (E-3 Sentry (AWACS), n.d.), AWACS is an airborne early warning and control platform designed to provide continuous surveillance, identify threats, and support coordinated decision-making through real-time transmission of monitored data. In the context of cross-border railway corridors, the relevance of AWACS lies not in direct military replication but in the transferable logic of multi-source sensing, real-time monitoring, and end-to-end visibility. A distributed sensing architecture that combines satellite observations, UAV-based surveillance, and ground-level sensors can create a unified information space around the corridor, enabling operators to detect both large-scale and localised anomalies. This logic is also reflected in NATO's AFSC concept, which aims to integrate air, land, space, and unmanned assets into a common surveillance and control environment (NATO, 2025). For railway applications, the theoretical value of AWACS therefore lies in its ability to support early anomaly detection, shorten the observe-orient phase, and improve the informational basis of C2 processes.

Although radar frequency bands and sensing technologies differ in their technical characteristics, their importance in this study is primarily conceptual rather than hardware-specific. Low-frequency, wide-area sensing provides broad surveillance coverage, while more localised radar and optical systems can enhance the protection of vulnerable assets such as bridges, tunnels, crossings, and marshalling areas (Besada et al., 2022; Bonin, 2025). The relevance of these technologies lies in their ability to enable layered detection, reduce blind spots, and strengthen the monitoring capacity of railway corridors under hybrid-threat conditions. Thus, the key theoretical contribution of the AWACS analogy is not a catalogue of radar solutions, but the argument that corridor preparedness requires fused, multi-layered, and real-time awareness rather than isolated monitoring tools.

The second pillar is Command and Control (C2), which transforms situational awareness into coordinated action. Based on NATO terminology, C2 may be

understood as the exercise of authority and direction over entrusted systems and resources to achieve a common objective. In cross-border railway corridors, this principle is relevant because digital resilience depends not only on sensing and communications but also on how responsibilities, escalation routes, and decisions are organised across institutions, infrastructure operators, and control levels (McDowell et al., 2024). Existing doctrine distinguishes among centralised, decentralised, and distributed architectures. For railway corridors exposed to failures, cyber incidents, and cross-border interoperability constraints, the most relevant insight is that resilience increases when coordination structures remain functional even under degraded communication conditions. In such systems, local autonomy, interoperability, and access to a shared operational picture become as important as central supervision.

The growing automation of C2 further reinforces the need to combine machine support with human oversight. Algorithmic solutions cannot replace human interpretation, strategic judgement, and creative decision-making, especially in complex and high-risk environments. Similarly, trust in automated systems depends on transparency, explainability, and the preservation of human responsibility in abnormal situations (McDowell et al., 2024). In the railway context, this means that digital C2 systems should support rather than replace operational personnel. Practical examples, such as Wabtec's Precision Dispatch System and the dual-control model of the Channel Tunnel, illustrate how digital coordination can improve continuity, throughput, and fault tolerance when supported by clear procedures and interoperable governance arrangements (Copan, 2020). Therefore, within the logic of this article, C2 constitutes the organisational layer of preparedness: it links sensing, communication, and response into a coherent management capability.

The third conceptual pillar is trust in software and digital components. Beyond observability and coordination, resilient corridor operation requires confidence that critical software and devices are authentic, protected, and restricted in their privileges. For this reason, the study draws on macOS security principles as an analogue for secure-by-design architecture in railway digital systems. Relevant mechanisms include Secure Enclave, System Integrity Protection, Gatekeeper, code signing, notarization, Sandboxing, and Transparency, Consent & Control (Li, 2007). Their theoretical significance lies not in platform-specific implementation details, but in the broader logic of root-of-trust, secure boot, integrity control, and least-privilege execution. In railway systems, this logic can be applied to controllers, onboard software, ETCS/RBC servers, and inter-system gateways to prevent unauthorised modification, restrict unsafe execution, and isolate compromised processes.

This interpretation is consistent with sector-specific cybersecurity standards. IEC 62443 requires industrial systems to verify the authenticity of software and firmware, apply segmentation, and control traffic between trust zones (Copan,

2020). Likewise, railway-oriented cybersecurity governance under CENELEC TS 50701 emphasises centrally managed protection against malicious code and the need for trusted software policies across interconnected transport environments (Lodi et al., 2026). Consequently, the relevance of macOS-derived principles in this article lies in their offering a clear conceptual model for software provenance, execution control, and segmentation in railway OT/IT systems. Rather than treating cybersecurity as an additional protective layer, this approach embeds trust directly into the architecture of digital operations.

The final conceptual pillar is communication continuity through LEO-based redundancy. Even well-monitored and securely configured railway systems remain vulnerable if communications fail. To address this problem, the study considers Starlink as a supplementary communication layer for critical railway applications. Its theoretical relevance lies in low-orbit architecture, comparatively low latency, and geographically diverse routing, which reduce reliance on single terrestrial communication paths (Ma et al., 2023; Tanveer et al., 2023). For corridor management, this means that LEO connectivity can serve as a fallback channel for telemetry, dispatching, and degraded-mode coordination in the event of an FRMCS outage, terrestrial disruption, or partial network failure. At the same time, Starlink's applicability is not unlimited: terrain, tunnels, vegetation, and line-of-sight constraints may reduce service stability in certain operating environments (Besada et al., 2022; Ma et al., 2023; Mohan et al., 2024). Thus, LEO connectivity should be understood as an additional layer of resilience rather than a universal substitute for terrestrial railway communications.

Building on these four elements, the study introduces the Preparedness Index (PI) as an integrative framework that converts technical and organisational conditions into measurable management variables. Conceptually, PI follows the logic of composite indicators used in recent resilience research, where diverse variables are normalised, weighted, and aggregated into a single interpretable score (Nickdoost et al., 2024). However, unlike climate-oriented or hazard-specific resilience indices, PI is tailored to hybrid-threat environments typical of cross-border railway systems. It comprises three complementary sub-indices: Technological Preparedness, Organisational Preparedness, and Operational Preparedness. Together, these dimensions allow the system to be assessed not only in terms of engineering performance, but also in terms of governance quality, response capability, and continuity under degraded conditions.

Within this structure, AWACS-inspired sensing primarily contributes to Technological Preparedness by improving detection coverage and reducing time-to-awareness. C2 architectures and institutional interoperability contribute to Organisational Preparedness by clarifying roles, decision rights, escalation pathways, and inter-agency coordination. Secure-by-design controls strengthen both Technological and Organisational Preparedness by formalising software

trust, segmentation, and execution integrity across distributed railway systems. LEO redundancy contributes primarily to Operational Preparedness by enabling fallback communication, maintaining continuity, and supporting response routines when terrestrial channels are compromised. In this sense, the PI does not treat these technologies as isolated innovations, but as measurable components of a broader preparedness architecture.

Recent transport resilience studies argue that effective assessment requires dynamic, multidimensional, and comparable measurement across performance, governance, and recovery functions (Connolly et al., 2026; Lodi et al., 2026). In line with this logic, the PI operationalises preparedness as a quantifiable state rather than a purely descriptive condition. It provides a structured way to link engineering KPIs with management decisions, enabling corridor operators and public authorities to identify weak points, prioritise interventions, and compare readiness across different nodes or segments. As a result, the theoretical contribution of this section is to establish a bridge among technological solutions, governance principles, and a composite preparedness metric that supports resilience-oriented decision-making in cross-border railway corridors.

2. Results

The MATLAB-based simulations of the PI framework provide clear quantitative evidence of how different layers of technological, organisational and operational measures influence corridor resilience under hybrid-threat conditions. Across all experiments, each executed in 20 independent runs to reduce scenario variance, the system displayed consistent patterns of degradation in the baseline configuration and substantial performance improvements when the complete resilience architecture was enabled.

In the baseline scenario, which lacked LEO redundancy, integrity verification, and advanced situational-awareness capabilities, communication disruptions reduced system availability by 17–23% and increased average recovery time by 28%. The results were relatively stable across runs (SD approx. 3–5%), suggesting that the system's vulnerability is robust to minor behavioural fluctuations. When LEO satellite redundancy (Starlink) and macOS-derived secure-by-design mechanisms were introduced, performance improved markedly: availability increased to 99.27%, packet loss fell to 0.11%, and recovery time decreased by 34%. These contrasts are summarised in Table 1, which provides a consolidated overview of both scenarios and highlights the practical magnitude of these improvements.

Table 1. Baseline vs. enhanced scenarios

Performance Metric	Baseline Scenario (no redundancy, no trust verification)	Enhanced Scenario (LEO redundancy + AWACS + macOS security)	Improvement, %	Simulation Context
System availability, %	82.5	99.27	+20.3	MATLAB model of corridor-level C2/SCADA topology
Mean delay, ms	265	174	–34.3	Communication latency during hybrid-threat event
Mean recovery time, s	12.8	8.4	–34.4	Restoration of service after FRMCS failure
Packet loss, %	0.69	0.11	–84.1	Data transmission reliability in degraded mode
Anomaly detection speed (relative)	1.00 (baseline)	1.42×	+42.0	AWACS algorithm with multi-sensor fusion
Unauthorised process attempts (count)	100	37	–63.0	macOS Secure Boot and Notarisation simulation
PI – Technological preparedness	0.67	0.89	+32.8	Normalised sub-index (KPI-based)
PI – Organisational preparedness	0.61	0.83	+36.1	SOP/C2 coordination efficiency
PI – Operational preparedness	0.58	0.81	+39.6	Training and response readiness
Composite preparedness index (PI)	0.62	0.84	+35.5	Weighted mean of three dimensions

Beyond basic communication stability, the integration of AWACS-type sensor-fusion algorithms demonstrated a measurable effect on situational awareness. Across simulations, anomaly detection latency decreased by approximately 42% (SD = 6.2%), primarily because the system began recognising irregular cross-domain patterns earlier. This earlier recognition subsequently shortened the decision-making timeline in C2-controlled environments. Figure 1 contrasts a conventional detection pipeline with an AWACS-augmented one, showing

improvements at nearly every stage of the detection-classification-decision sequence.

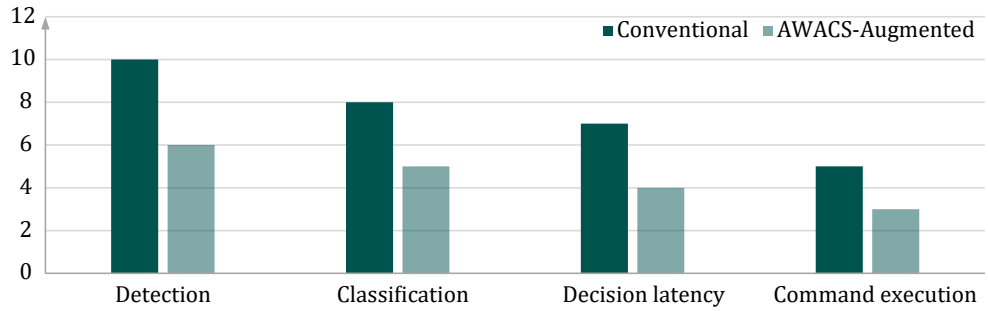

Figure 1. Comparative detection and response timelines

A similar pattern emerges when analysing the impact of secure-by-design mechanisms. Without integrity controls, the simulated SCADA/ERTMS architecture registered an average of 100 unauthorised process attempts per cycle. Enabling secure boot, code notarisation, and trust verification reduced this value to 37 attempts, representing a 63% reduction. Meanwhile, the system's ability to isolate malicious processes, as measured by containment efficiency, increased from 54% to 88%. These results indicate that security design choices are not merely defensive add-ons but active contributors to operational continuity, as shown in Figure 2.

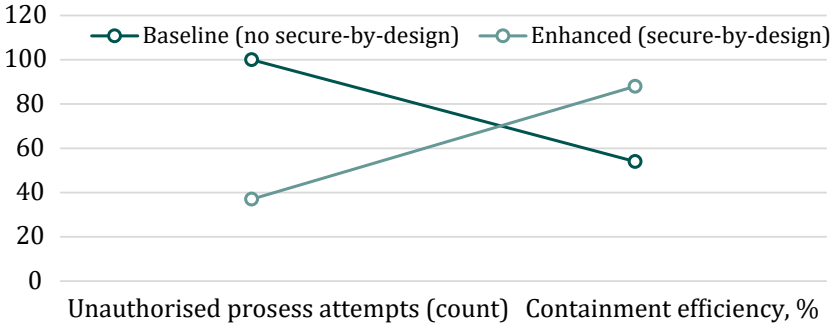

Figure 2. Impact on intrusion frequency and containment efficiency

The application of the PI framework highlights resilience as a multidimensional and interdependent construct. The Technological Preparedness sub-index increased from 0.67 to 0.89, reflecting improvements in redundancy, latency stability, and

protocol-level interoperability. Organisational Preparedness rose from 0.61 to 0.83 due to clearer C2 roles, SOP standardisation and the adoption of trust-policy enforcement. Operational Preparedness increased from 0.58 to 0.81 as faster detection-to-action cycles were achieved and fallback communication mechanisms were validated. The full breakdown of these sub-indices is presented in Table 2, which illustrates not only the magnitude of change but also the relative balance across the three PI dimensions.

Table 2. Preparedness index sub-scores before and after framework integration

Preparedness Dimension	Baseline Score (no redundancy, limited SOP, no trust layer)	Enhanced Score (LEO redundancy + AWACS + SOP maturity + secure-by-design)	Improvement, %	Notes (Simulation Context)
Technological preparedness	0.67	0.89	+32.8	Based on availability, latency, loss, recovery time, interoperability
Organisational preparedness	0.61	0.83	+36.1	SOP maturity, C2 clarity, coordinated governance, software trust policies
Operational preparedness	0.58	0.81	+39.6	Exercises, detection-to-action time, fallback comms readiness
Composite PI score	0.62	0.84	+35.5	Weighted aggregate of 3 sub-indices (normalised)

To understand how PI translates into real operational resilience, we analysed corridor performance under partial loss of connectivity. A strong positive relationship was found between PI scores and interoperability outcomes derived from the TAF/TAP TSI and RINF models. Systems with PI values above 0.80 maintained stable cross-system data exchange and dispatch coordination, with deviations kept under 10 seconds. However, nodes with PI below 0.60 experienced cascading delays and intermittent message rejection events, indicating structural fragility. This correlation is visualised in Figure 3, which plots PI values against interoperability performance and highlights the practical threshold at which the system transitions from vulnerability to functional stability.

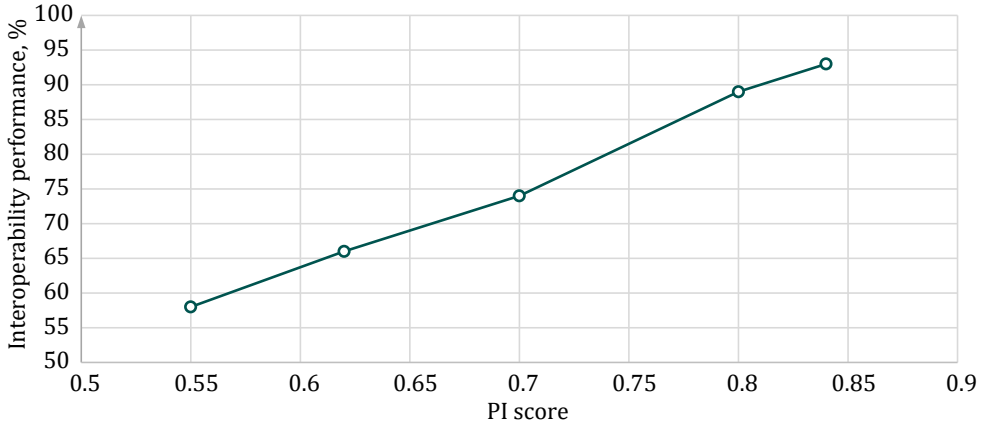

Figure 3. Correlation between PI and interoperability

Taken together, these results confirm that the PI framework captures not only technical performance but also the interplay among organisational rules, communication architectures, and operational routines. The combination of AWACS-style awareness, LEO redundancy, and secure-by-design software principles forms a coherent resilience layer that materially increases the robustness of cross-border railway corridors against hybrid threats.

3. Discussion

The results of this study show that preparedness in cross-border railway corridors should be understood not as a fixed state of technical robustness, but as a dynamic capability emerging from the coordinated functioning of sensing systems, communication redundancy, trust architectures, and organisational governance. The PI proposed in this research provides a structured means of integrating these elements by translating classical engineering indicators availability, delay, recovery time, and packet loss into a management-oriented framework. This interpretation aligns with recent resilience-engineering insights demonstrating that composite, multi-dimensional indices outperform single-variable measures when assessing real-world system behaviour (Agyeman & Fiase, 2026).

A central insight from the simulations is the mutually reinforcing interaction between the three PI sub-indices. When AWACS-inspired situational awareness, LEO satellite redundancy, and secure-by-design controls were introduced, not only did Technological Preparedness increase (e.g., a 34% reduction in recovery

time and a drop in packet loss to 0.11%), but these gains cascaded into stronger Organisational and Operational Preparedness. This observation is consistent with broader resilience research showing that institutional clarity, coordination rules, and SOP maturity often shape recovery trajectories as strongly as the underlying physical or digital infrastructure (Johnson, 2023). The simulations reinforce these findings: improved anomaly detection through AWACS-type multi-source fusion accelerated C2 decision cycles, thereby enabling earlier SOP activation and more stable operational behaviour.

A further contribution arises from the integration of macOS-derived secure-by-design principles, such as secure boot, code signing, notarisation, sandboxing and TCC control, which reduced unauthorised process attempts by 63% in the simulated SCADA/ERTMS architecture. This demonstrates how commercial cybersecurity architectures can be adapted to industrial and transport environments, complementing sector-specific standards such as CENELEC TS 50701 and IEC/ISA 62443. Similar conclusions have been reached in recent work on cyber-physical systems, where software-trust architectures are increasingly recognised as indispensable prerequisites for operational safety and resilience (Agyeman & Fiase, 2026).

The role of Starlink's LEO redundancy is equally noteworthy. Its ability to stabilise availability at 99.27% and offset terrestrial outages corroborates emerging evidence that multi-constellation LEO systems can meaningfully enhance communication continuity for critical infrastructure (Mohan et al., 2024; Tanveer et al., 2023). Complementary studies on free-space optical and hybrid satellite-ground architectures likewise emphasise their value in maintaining service reliability in environments exposed to disruption (Ma et al., 2023).

Collectively, these results offer a theoretical contribution: resilience in cross-border railway corridors is best conceptualised as a *quantifiable preparedness state* rather than a static condition. This situates the PI within a broader shift toward anticipatory governance and continuous, indicator-driven monitoring in resilience research (Tafur et al., 2025; Nickdoost et al., 2024).

Despite the positive performance patterns, the findings also highlight clear structural constraints. Even corridors equipped with strong technological redundancy and secure-by-design enforcement performed poorly when organisational maturity was low, for instance, when SOP alignment, escalation logic or cross-border data-sharing protocols were inconsistent. This supports long-standing systems-theory perspectives suggesting that resilience failures often originate from misalignment between interconnected components rather than the malfunction of any single subsystem (Mohan et al., 2024; Tanveer et al., 2024).

To translate these analytical findings into practical implications, several areas for policy intervention become evident. The following recommendations highlight

where decision-makers can act most effectively to strengthen preparedness across the EU-Ukraine corridor operations outlined below.

1. Standardisation of Preparedness Measurement. The PI provides a unified method for EU-Ukraine corridor partners to establish measurable preparedness thresholds.
2. Targeted Investment. Because the PI decomposes preparedness into three distinct dimensions, it allows precise identification of the most impactful upgrades (e.g., sensors vs. redundancy vs. SOP alignment).
3. Institutional Interoperability Requirements. The results show that SOP and governance alignment must be treated not merely as administrative processes but as quantitatively measurable components of interoperability.
4. Integration into EU Resilience Programs. The PI could support resilience assessment and monitoring within TEN-T, Solidarity Lanes and NATO AFSC-aligned initiatives.

These considerations illustrate how the PI can be operationalised within real-world governance structures and used to guide investment choices, interoperability commitments and resilience monitoring practices. At the same time, they underscore that preparedness evolves continuously, shaped by technological change, shifting hybrid-threat landscapes and institutional dynamics. Recognising this opens several avenues for further study:

- Field calibration using real ERTMS/SCADA/RBC telemetry;
- Human-in-the-loop modelling for degraded-mode decision performance;
- Expanded AWACS fusion testing on actual border infrastructure;
- Digital twin integration for predictive preparedness analytic;
- Organisational network modelling (data-sharing asymmetries, protocol mismatch).

Advancing research in these directions would allow the PI framework to be refined, empirically validated, and expanded into a tool capable of real-time monitoring and predictive analysis. Strengthening its empirical foundation will also support more accurate prioritisation of interventions and more reliable benchmarking of preparedness across jurisdictions. Ultimately, deepening the PI's methodological base will help institutions anticipate disruptions more effectively, coordinate responses with greater precision, and sustain corridor functionality under increasingly complex hybrid-threat conditions.

Conclusions

This research develops and validates a novel PI that positions resilience in cross-border railway corridors not as a static technical attribute, but as a measurable, adaptive capability grounded in technological redundancy, organisational

governance, and operational readiness. By consolidating these three dimensions, Technological Preparedness, Organisational Preparedness, and Operational Preparedness into a unified composite indicator, the PI enables both high-level strategic assessment and fine-grained diagnostic analysis of preparedness under hybrid-threat conditions. This integrated view marks a departure from traditional infrastructure assessments that rely on isolated metrics, offering instead a systemic measurement approach that aligns with contemporary resilience theory and anticipatory governance frameworks.

The simulation results reinforce the value of this multidimensional approach. The incorporation of AWACS-type situational awareness significantly accelerated anomaly detection and shortened the observe-orient-decide loop in C2 processes. Starlink-based LEO redundancy proved critical in stabilising availability and mitigating packet loss during terrestrial communication failures, which increasingly define modern hybrid-threat environments. Equally importantly, the application of macOS-derived secure-by-design principles such as secure boot, code signing, notarisation, sandboxing, and TCC controls dramatically reduced unauthorised process attempts within SCADA/ERTMS architectures. Collectively, these findings demonstrate that resilience emerges not solely from hardware robustness or network design, but from the orchestration of sensing, communication, trust, and governance mechanisms.

The PI therefore contributes both theoretically and practically. Theoretically, it advances resilience research by embedding management-oriented constructs, SOP maturity, escalation logic, and institutional coordination directly into technical architectures. This framing supports recent arguments that socio-technical misalignments, rather than isolated equipment failures, often determine the severity and duration of disruptions in critical infrastructure systems. In practice, the PI offers a structured pathway for embedding EU and NATO standards, including EN 50126/50128/50129, CENELEC TS 50701, and IEC/ISA 62443 into preparedness evaluation, enabling corridor operators and policymakers to benchmark readiness against consistent, interoperable criteria.

The PI provides a governance tool that can inform interoperability agreements within the EU-Ukraine rail corridor, guide targeted investments under programmes such as TEN-T and Solidarity Lanes, and support future integration with NATO's AFSC vision for distributed situational awareness. By translating technical performance into actionable management indicators, the PI bridges the gap between engineering reliability and institutional decision-making, an area repeatedly identified as critical for sustaining network continuity during crises.

Despite the promising results, several limitations warrant further exploration. The simulations relied on standardised network assumptions and synthetic failure scenarios; real-world operational environments may introduce additional asymmetries, latency dynamics, and organisational frictions that the model does not

capture. Additionally, the current weighting structure of the PI, while grounded in empirical relationships observed in the simulations, would benefit from validation through multi-criteria decision-making techniques such as Best-Worst Method (BWM) or fuzzy extensions.

Future research should therefore prioritise longitudinal field validation using real telemetry from ERTMS, SCADA and RBC systems, as well as expanding AWACS-based multi-source fusion testing on actual border infrastructure. Integrating the PI with digital twin architectures would also enable predictive preparedness analytics, supporting proactive rather than reactive corridor management. Finally, modelling organisational networks, particularly data-sharing asymmetries and protocol mismatches, would deepen understanding of how cross-jurisdictional coordination affects preparedness outcomes.

The Preparedness Index developed in this study provides a robust conceptual and operational foundation for enhancing the resilience of cross-border railway corridors facing increasingly complex hybrid threats. By unifying sensing technologies, secure communication architectures, software trust mechanisms, and institutional governance into a single evaluative structure, the PI offers a practical pathway toward more anticipatory, secure, and interoperable European transport systems.

Disclosure Statement

The authors declare no conflict of interest.

Statement of the Use of Generative AI and AI-assisted Technologies in the Writing Process

The writers did not utilize AI-assisted technologies or generative AI during the writing process.

REFERENCES

Agyeman, P., & Fiase, D. (2026). Cybersecurity and resilience capabilities in transport systems: Assessing frameworks, gaps, and an integrated maturity model. *Asian Journal of Computing and Engineering Technology*, *7*(1), 1–19. https://doi.org/10.47604/ajcet.3658

Besada, J. A., Campaña, I., Carramiñana, D., Bergesio, L., & de Miguel, G. (2022). Review and simulation of counter-UAS sensors for unmanned traffic management. *Sensors*, *22*(1), Article 189. https://doi.org/10.3390/s22010189

Bonin, A. (2025). The impact of the Ukraine war on European cybersecurity policies and legislation for critical infrastructure, including energy. In A. Barichella, & J. Yada (Eds.),

The Palgrave Handbook of Cybersecurity, Technologies and Energy Transition (pp. 1–40). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-04196-9_31-1

Connolly, L., de Paor, C., Micu, A., & O'Connor, A. (2026). Resilience of transport and associated infrastructure to climate, cyber and physical threats. *TRAconference 2024. Lecture Notes in Mobility* (pp. 223–229). Springer, Cham. https://doi.org/10.1007/978-3-032-04774-8_33

Copan, W. (2020). *Security and privacy controls for information systems and organizations*. NIST Special Publication 800-53. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

E-3 Sentry (AWACS). (n.d.). https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104504/e-3-sentry-awacs/

EU-Ukraine Solidarity Lanes. (n.d.). https://transport.ec.europa.eu/ukraine/eu-ukraine-solidarity-lanes_en

Johnson, J. (2023). Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age. *Defence Studies*, *23*(1), 43–67. https://doi.org/10.1080/14702436.2022.2102486

Kharrat, N., Hamani, N., Benaissa, M. Benaissa, M., & Kermad, L. (2025). Building sustainable and resilience index for assessing freight transport. *Environment, Development and Sustainability*, 1–21. https://doi.org/10.1007/s10668-025-06630-5

Klepper, D. (2025, May 22). Russian hackers target firms shipping aid to Ukraine, US intelligence says. Retrieved May 6, 2026, from AP News: https://apnews.com/article/russia-cyberattack-ukraine-aid-nsa-6308ca3e11c8299470df573e4f422878

Li, A. (2007, December 2007). RFC 5109 – RTP payload format for generic forward error correction. Retrieved May 6, 2026, from https://datatracker.ietf.org/doc/html/rfc5109

Lodi, C., Cheimariotis, I., Stępniak, M., Gkoumas, K., dos Santos, F. M., Grosso, M., & Marotta, A. (2026). Quantitative and qualitative assessment of European research and innovation initiatives in transport resilience. *Transport Research Arena (TRA) in Dublin, Ireland. Lecture Notes in Mobility* (pp. 409–415). Springer, Cham. https://doi.org/10.1007/978-3-032-04774-8_60

Ma, S., Chou, Y. C., Zhao H., Chen L., Ma, X., & Liu, J. (2023). Network characteristics of LEO satellite constellations: A Starlink-based measurement from end users. *IEEE INFOCOM 2023 – IEEE Conference on Computer Communications*, New York City, NY, USA, 1–10. https://doi.org/10.1109/INFOCOM53939.2023.10228912

McDowell, K., Novoseller, E., Madison, A., Goecks, V. G., & Kelshaw, C. (2024). Re-envisioning command and control. *2024 International Conference on Military Communication and Information Systems (ICMCIS)*, Koblenz, Germany, 1–7. https://doi.org/10.1109/ICMCIS61231.2024.10540901

Mohan, N., Ferguson, A. E., Cech, H., Bose, R., Renatin, P. R., Marina, M. K., & Ott, J. (2024). A multifaceted look at Starlink performance. *ACM Web Conference 2024*, 2723–2734. https://doi.org/10.1145/3589334.3645328

NATO. (2025, December 10). *Deterrence and defence*. https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence

NATO. (2026, March 03). *AWACS: NATO's 'eyes in the sky'*. https://www.nato.int/en/what-we-do/deterrence-and-defence/awacs-natos-eyes-in-the-sky?selectedLocale

Nickdoost, N., Shooshtari, M. J., Choi, J., Smith, D., & AbdelRazig, Y. (2024). A composite index framework for quantitative resilience assessment of road infrastructure systems. *Transportation Research Part D: Transport and Environment*, *131*, Article 104180. https://doi.org/10.1016/j.trd.2024.104180

Tafur, C. L., Camero, R. G., Rodríguez, D. A., Rincón, J. C. D., & Saenz, E. R. (2025). Applications of artificial intelligence in air operations: A systematic review. *Results in Engineering*, *25*, Article 103742. https://doi.org/10.1016/j.rineng.2024.103742

Tanveer, H. B., Puchol, M., Singh, R., Bianchi, A., & Nithyanand, R. (2023). Making sense of constellations: Methodologies for understanding Starlink's scheduling algorithms. *CoNEXT 2023: The 19th International Conference on emerging Networking EXperiments and Technologies*, Paris, France, 37–43. https://doi.org/10.1145/3624354.3630586

Tanveer, H., Adam, M. A., Khan, M. A., Ali, M. A., & Shakoor, A. (2024). Analyzing the performance and efficiency of machine learning algorithms, such as Deep Learning, Decision Trees, or Support Vector Machines, on various datasets and applications. *The Asian Bulletin of Big Data Management*, *3*(2), 126–136. https://doi.org/10.62019/abbdm.v3i2.83