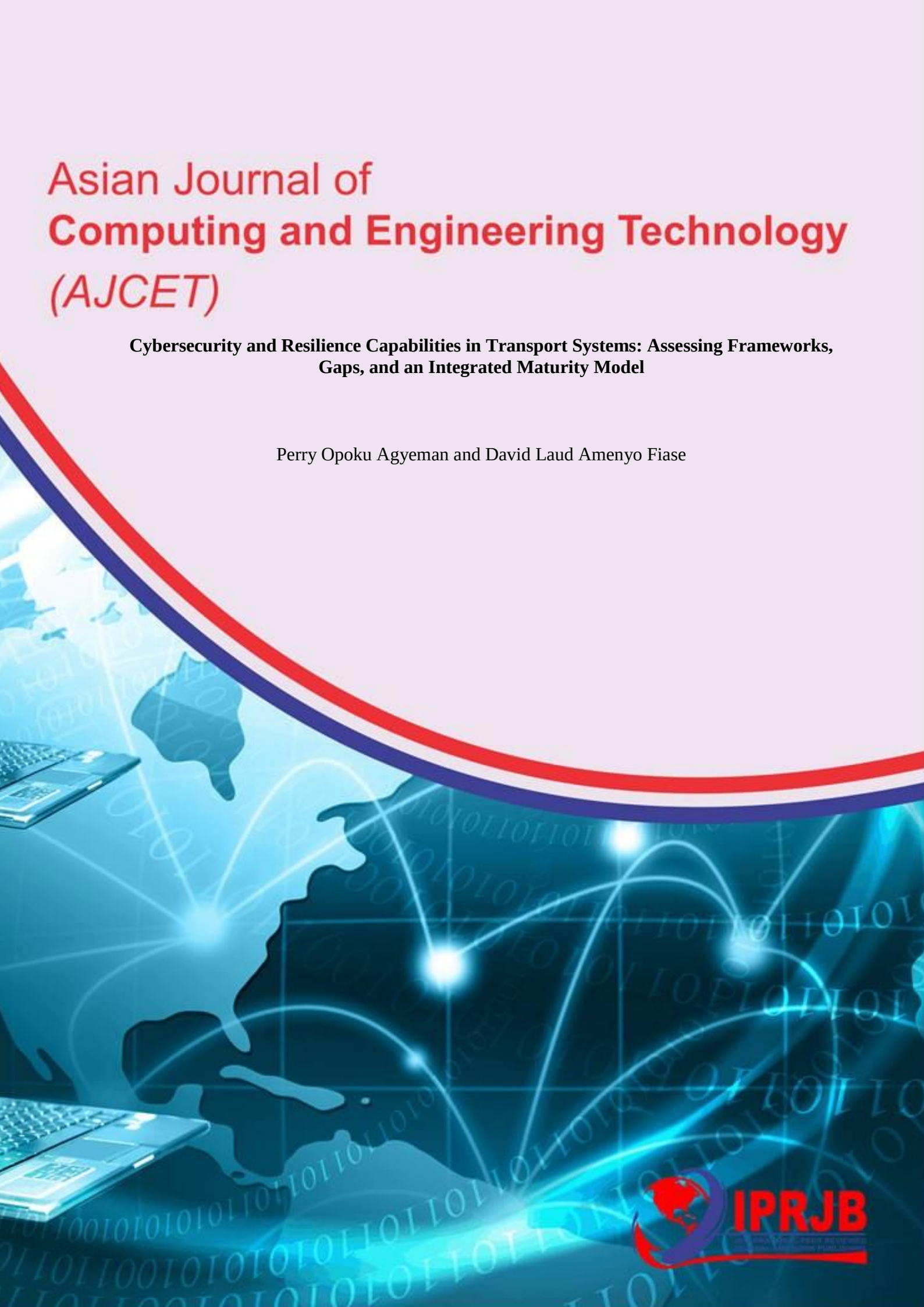
Asian Journal of
Computing and Engineering Technology
(AJCET)

Cybersecurity and Resilience Capabilities in Transport Systems: Assessing Frameworks, Gaps, and an Integrated Maturity Model

Perry Opoku Agyeman and David Laud Amenyo Fiase



Asian Journal of Computing and Engineering Technology
ISSN 2959-1775 (online)
Vol.7, Issue 1 No.1, pp 1 - 19, 2026

www.iprjb.org

Cybersecurity and Resilience Capabilities in Transport Systems: Assessing Frameworks, Gaps, and an Integrated Maturity Model

[1]Perry Opoku Agyeman
Regent University College of Science and Technology, Accra-Ghana

[2]David Laud Amenyo Fiase
Regent University College of Science and Technology, Accra-Ghana

Article History

Received 19th December 2025

Received in Revised Form 25th January 2026

Accepted 24th February 2026

How to cite in APA format:

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

Abstract

Purpose: Transport systems are increasingly digital, exposing them to complex cybersecurity risks that threaten operational continuity and public safety, prompting this study to evaluate and enhance cybersecurity and resilience capabilities across transport networks through analysis of major frameworks from National Institute of Standards and Technology, International Organization for Standardization, and European Union Agency for Cybersecurity.

Methodology: Using a mixed-method approach that combined documentary analysis, expert interviews, and a pilot resilience maturity assessment across aviation, rail, maritime, and road sectors,

Findings: The study identified uneven preparedness levels, with aviation demonstrating stronger monitoring and recovery mechanisms while road transport showed weaker incident response coordination. Significant gaps were found in data-sharing practices, workforce awareness, and cross-sector policy alignment. In response, a Cybersecurity Resilience Maturity Model (CRMM) structured around Prevention, Detection, Response, Recovery, and Adaptation was developed to support benchmarking, guide investment decisions, and monitor resilience improvement.

Unique Contribution to Theory, Practice and Policy: The study concludes that integrated cybersecurity–resilience strategies are essential for ensuring safe, reliable, and sustainable transport operations in an increasingly connected environment.

Keywords: *Cybersecurity, Transport Systems, Resilience Maturity Model, Critical Infrastructure Protection, Risk Management, Digital Resilience*

INTRODUCTION

The evolution of transport systems into digitally enabled, interconnected platforms has brought major operational benefits and serious vulnerabilities. Modern infrastructure such as intelligent transport systems (ITS), autonomous vehicles, connected logistics platforms, and cloud-based control networks have transformed the way highways, railways, ports, and urban transit operate (Knyazkina, Khamitov, & Chernikova, 2024). These advancements deliver higher efficiency and responsiveness but also expand the "attack surface" of critical transport infrastructure. As networks evolve into complex cyber-physical systems, they become prime targets for sophisticated cyber assaults capable of disrupting service continuity, compromising safety, and inflicting economic damage (Rossiter, 2025).

Experience has shown that transport operations are no longer purely mechanical or physical; they are deeply embedded in information technology and communications. For instance, malware or ransomware attacks on metro networks, GPS spoofing affecting navigation systems, or manipulation of industrial control systems now pose threats not only to assets, but to travelers, cargo, and supply chains. The cascading effect of a cyber-incident in one mode of transport say rail can ripple through multi-modal operations, affecting aviation, road freight, and maritime logistics (Di Zhang et al., 2024). These developments underscore the urgency of enhancing both cybersecurity and resilience capabilities within the transport sector.

Cybersecurity and resilience are closely related but conceptually distinct. Cybersecurity typically emphasizes preventing, detecting, and responding to unauthorized access, data breaches, or system compromise. Resilience, by contrast, emphasizes an infrastructure's capacity to withstand, recover and adapt from adverse events (Belokas, Saroglou, Moschovou, & Vlahogianni, 2024). In transport systems, resilience extends beyond protection of assets to include rapid restoration of service, adaptive response to evolving threats, and institutional learning post-incident. Many existing frameworks such as ISO 27001 (Information Security Management) or the NIST Cybersecurity Framework (Identify Protect Detect Respond Recover) apply strong controls over prevention and detection, but give limited guidance on system recovery, adaptation, and continuity in a dynamic operational environment (Rossiter, 2025). This gap highlights a structural limitation: protective mechanisms without resilience planning leave transport infrastructure exposed to inevitable disruptions.

In contemporary transport, the convergence of operational technology (OT) and information technology (IT) further amplifies risk. IT systems those handling data, connectivity, cloud services typically have standard encryption, monitoring and patching protocols. OT systems sensors, programmable logic controllers (PLCs), signaling hardware frequently use legacy protocols with weak or no authentication and long lifecycles (Knyazkina et al., 2024). When OT and IT networks are interconnected without proper segmentation, legacy OT becomes a gateway for adversaries into broader operational networks. The result is a heterogeneous environment where a weakness in one subsystem may compromise the entire transport ecosystem. Such vulnerabilities not only threaten technical performance, but raise public-safety, national-security and economic-resilience concerns (Belokas et al., 2024).

While prevention remains critical, recent scholarly work emphasizes resilience as a key determinant of long-term performance of critical transport systems. For example, Di Zhang et al. (2024) in their systematic review of maritime transport networks argue that resilient infrastructure is one that can restructure, recover and continue operations despite significant shocks. Similarly, Rossiter (2025) explores the evolving cyber-threats at "smart airports" and

shows that the ability to recover and adapt often matters more than the ability simply to block every potential attack. These shifts reflect a broader consensus: in highly interconnected, digital-enabled transport infrastructures, absolute protection is unattainable, making resilience a strategic imperative.

Despite growing awareness, a significant challenge persists: the absence of a standardized method to assess and benchmark resilience maturity across multimodal transport systems. Many transport organizations adopt cybersecurity frameworks primarily to meet regulatory or compliance requirements, rather than as part of a strategic resilience posture. As a result, they lack metrics to gauge their ability to detect disruptions, restore services, adapt to change, and learn from experience. Without measurable indicators, organizations struggle to assess readiness or benchmark progress against sectoral best practices (Knyazkina et al., 2024). This gap is particularly acute across transport modes road, rail, maritime and aviation where cybersecurity implementations vary widely, governance structures differ, and operational cultures diverge.

Given this context, the present study aims to evaluate and strengthen cybersecurity and resilience capabilities in transport systems by analyzing existing frameworks, assessing maturity of resilience, identifying systemic gaps, and developing an integrated model tailored to transport infrastructure. Specifically, the research introduces a "Cybersecurity-Resilience Maturity Model" (CRMM) built on international standards and underpinned by dynamic learning and adaptive governance. The model offers transport organizations a structured approach to benchmark and incrementally improve their resilience maturity across technical, organizational and operational dimensions.

By addressing governance, technology integration and incident-response coordination, this research contributes to advancing cyber-resilient transport infrastructure. The resulting insights target policymakers, system engineers and transport operators, guiding the development of adaptive cybersecurity strategies that sustain operational continuity, protect public safety and preserve digital trust. Positioned at the intersection of cybersecurity engineering, resilience management and critical-infrastructure protection, this study addresses an ecosystem increasingly vital to national and global transport security.

In referencing this to the NIST Cybersecurity Framework, the function models are limited to originally five namely: Identify, Protect, Detect, Respond, and Recover. However, by the time of a 2026 study, the release of NIST CSF 2.0 by the National Institute of Standards and Technology had formally introduced the additional Govern function to strengthen risk oversight, accountability, and strategic alignment. The failure to incorporate this updated framework renders the analysis of existing cybersecurity structures technically outdated, particularly in a sector such as transport where governance, regulatory coordination, and organizational responsibility are central to resilience. Consequently, the omission weakens the conceptual foundation of the framework comparison and limits the study's alignment with current best practices in cybersecurity governance and resilience planning.

Problem Statement

Despite the rapid digitalization of global transport systems, cybersecurity and resilience capabilities remain undermined by several persistent challenges, including fragmented cybersecurity practices across different transport modes, limited integration between cybersecurity measures and broader resilience management, ongoing vulnerabilities linked to

legacy operational technology (OT) systems, the absence of a standardized maturity assessment model to benchmark preparedness, and the potential for severe operational and socio-economic consequences resulting from cyber incidents.

The core problem, therefore, lies in the absence of a unified cybersecurity–resilience maturity model tailored to the unique dynamics of transport systems one that holistically addresses protection, adaptation, and recovery within a single framework.

Research Aim and Objectives

Aim

To evaluate and enhance cybersecurity and resilience capabilities in transport systems through analysis of existing frameworks, risk assessment models and technological safeguards.

Objectives

1. To analyze existing cybersecurity frameworks and their applications within transport infrastructure.
2. To assess the resilience capabilities of transport systems in responding to and recovering from cyber-threats.
3. To identify critical gaps in cybersecurity policies, technologies and incident response mechanisms across the transport sector.
4. To develop an assessment model for measuring cybersecurity resilience maturity in transport systems.
5. To propose an integrated framework that enhances both cybersecurity and resilience capabilities within transport networks.

Research Questions

This study seeks to answer the following research questions:

- What cybersecurity frameworks are currently implemented across transport systems, and how effectively do they address emerging threats?
- How resilient are transport systems in responding to, absorbing, and recovering from cyber incidents?
- What are the major gaps in cybersecurity policies, technologies, and incident response mechanisms within the transport sector?
- How can the maturity of cybersecurity resilience be assessed and measured across different modes of transport?
- What integrated framework can be developed to strengthen both cybersecurity and resilience capabilities in transport networks?

LITERATURE REVIEW

Theoretical Review

Cybersecurity Concepts

Cybersecurity is grounded in the Confidentiality, Integrity, and Availability (CIA) triad, which forms the foundation for protecting information and operational systems within digital infrastructures.

- Confidentiality: Ensures that sensitive information is accessible only to authorized individuals or systems, preventing data breaches and unauthorized disclosures (Srinivas et al., 2019).
- Integrity: Maintains the accuracy and reliability of data, ensuring that it is not altered maliciously or accidentally during transmission or storage.
- Availability: Guarantees that networks, systems, and data remain accessible and operational when needed for legitimate purposes, ensuring service continuity within critical sectors such as transport.

A supporting concept, defense-in-depth, complements the CIA triad by layering multiple security mechanisms such as encryption, firewalls, authentication controls, and network segmentation to create overlapping protection that limits the success of cyberattacks (Alcaraz & Lopez, 2018).

Transport System Vulnerabilities

The digital transformation of transport systems has improved efficiency but also introduced significant cybersecurity risks due to system interconnectivity and legacy infrastructure.

- SCADA Systems: Supervisory Control and Data Acquisition (SCADA) platforms manage real-time operations in rail, aviation, and maritime systems but often rely on outdated communication protocols with limited encryption and authentication, exposing them to unauthorized access (Macaulay & Singer, 2018).
- IoT Sensors: Connected devices collect data for vehicle monitoring, signaling, and logistics, yet weak encryption and insecure interfaces make them vulnerable to exploitation.
- GPS Manipulation: Jamming or spoofing GPS signals can mislead navigation and tracking systems, potentially compromising passenger and cargo safety (Humayed et al., 2017).
- Data Integrity Threats: Unauthorized alteration of transmitted data between control systems and field units can cause false readings, incorrect responses, or service failures.

These vulnerabilities reveal that cyber threats to transport systems are not isolated incidents but interconnected risks that can undermine both safety and reliability.

Resilience Theory

Resilience theory extends beyond conventional cybersecurity by emphasizing a system's ability to withstand, adapt to, and recover from disruptions. Its four core components are:

- Robustness: The strength of infrastructure to resist disruptions without performance degradation.
- Redundancy: Availability of alternative subsystems or pathways that ensure continuity of critical operations during disruptions.
- Recovery: The ability to restore normal functionality promptly after an incident.
- Adaptability: The capacity to learn from previous disruptions and improve future performance (Linkov & Trump, 2019).

In transport systems, resilience ensures that even when cyber incidents occur, operations can continue with minimal impact and be restored efficiently afterward.

Integration Gap: Cybersecurity and Resilience

A major shortfall in existing approaches is the separation between cybersecurity management and resilience planning.

- Traditional Approach: Cybersecurity typically emphasizes prevention and detection of attacks, focusing on compliance and perimeter defense.
- Resilience Approach: Concentrates on maintaining and restoring functionality but may overlook ongoing cyber threats and evolving adversarial tactics.
- Integration Need: Sustainable transport protection requires merging cybersecurity's proactive defense with resilience's adaptive recovery mechanisms (Smith & Woods, 2020).

An integrated framework would allow transport systems to not only prevent attacks but also recover rapidly and learn from incidents, strengthening long-term operational continuity and safety.

To address the safety–security nexus, it can be said that safety- a core theoretical pillar alongside resilience, recognized in land-based transport systems particularly rail and road—cybersecurity is increasingly embedded within the broader domain of functional safety. Traditionally, transport safety frameworks governed by bodies such as the International Organization for Standardization have focused on preventing system failures that could lead to physical harm, with cybersecurity now emerging as a critical threat vector capable of triggering unsafe states. The current separation between cybersecurity risk management and safety engineering undermines holistic system protection, as cyber incidents can directly compromise signaling systems, vehicle controls, traffic management platforms, and emergency response functions. Integrating safety as a foundational pillar alongside resilience therefore reframes cybersecurity not merely as an IT concern but as a core component of safe system operation, ensuring that cyber risk mitigation is embedded within hazard analysis, system design, operational controls, and recovery planning. This approach strengthens the conceptual model by aligning cybersecurity, safety assurance, and resilience into a unified framework capable of protecting both digital assets and human life across land-based transport infrastructure.

To enhance the theoretical depth of the Resilience section, the study would be strengthened by incorporating insights from Charles Perrow through his Normal Accident Theory, most prominently articulated in Normal Accidents: Living with High-Risk Technologies. This theory argues that in tightly coupled and complex systems such as modern rail and road transport infrastructures failures are not anomalies but inevitable outcomes of system interactions, a reality that is increasingly amplified by digital interdependencies and cyber-physical integration. Applying this lens reinforces the necessity of resilience not merely as recovery capacity but as a systemic design principle focused on anticipating, absorbing, and adapting to inevitable disruptions. By acknowledging that cyber incidents will occur despite preventive controls, the resilience framework shifts toward continuous monitoring, adaptive response, and organizational learning, thereby providing a stronger conceptual justification for the development of a maturity model aimed at managing complexity-driven risk rather than pursuing unrealistic zero-failure objectives.

Theoretical Frameworks

Several frameworks guide the implementation of cybersecurity and resilience strategies within critical infrastructure. However, their effectiveness varies when applied to complex and

interconnected transport systems. This section discusses the most relevant theoretical frameworks and highlights their strengths and limitations.

NIST Cybersecurity Framework (CSF)

Developed by the U.S. National Institute of Standards and Technology, the CSF provides a structured approach to managing cybersecurity risk through five core functions:

- Identify: Understand system assets, data, and vulnerabilities.
- Protect: Implement safeguards to secure critical functions.
- Detect: Monitor systems to identify anomalies and security events.
- Respond: Establish processes to contain and mitigate cyber incidents.
- Recover: Restore affected systems and improve resilience.

Relevance: The CSF offers flexibility and scalability, making it suitable for diverse sectors. For transport systems, it helps align technical security controls with risk management.

Limitation: It primarily emphasizes risk identification and response, offering limited guidance on operational resilience and adaptive recovery in dynamic transport environments (NIST, 2018).

ISO/IEC 27001 and ISO 22301 Standards

- ISO/IEC 27001: Focuses on establishing an Information Security Management System (ISMS) through structured control of data confidentiality, integrity, and availability.
- ISO 22301: Addresses Business Continuity Management (BCM), ensuring that organizations can continue essential functions during disruptions.

Relevance: Both standards provide an integrated approach to cybersecurity and continuity planning. Their systematic and auditable structure supports compliance and organizational accountability.

Limitation: These standards are process-oriented and often lack sector-specific adaptation for the complex, interconnected nature of transport networks (ISO, 2021).

ENISA Transport Sector Cybersecurity Guidelines

The European Union Agency for Cybersecurity (ENISA) developed sector-specific guidance for road, rail, aviation, and maritime systems.

- Focuses on critical asset identification, incident reporting, and cross-border coordination.
- Promotes harmonized cybersecurity measures and information sharing among stakeholders.

Relevance: ENISA's framework is practical for transport infrastructure as it integrates both technical and governance perspectives.

Limitation: It is mostly policy-driven and may not fully capture the operational dynamics and resilience maturity needed for real-time system recovery (ENISA, 2022).

Resilience Engineering Frameworks and the Resilience Matrix Model

- These frameworks emphasize anticipation, absorption, recovery, and adaptation as key resilience functions.

- The Resilience Matrix Model links technical, organizational, and cognitive dimensions of resilience to assess system robustness (Linkov & Trump, 2019).

Relevance: They provide a holistic view of system performance under stress, applicable to transport systems facing both cyber and physical disruptions.

Limitation: While strong in conceptual clarity, these models often lack specific operational metrics for cybersecurity implementation.

Cyber-Resilience Engineering Framework (CREF)

Developed by NIST, CREF combines traditional cybersecurity measures with resilience principles.

- Promotes adaptive capacity and continuous improvement in response to evolving cyber threats.
- Encourages integration between IT and operational technology (OT) environments.

Relevance: CREF's system-level perspective aligns closely with transport networks that depend on interlinked digital and physical assets.

Limitation: Its adoption in transport contexts remains limited due to the absence of standardized tools for measuring resilience maturity (NIST, 2021).

Summary of Overlaps and Limitations

- Most frameworks emphasize protection and risk management but give limited attention to adaptive recovery.
- Few frameworks integrate cybersecurity with operational resilience in a transport-specific context.
- There is a need for a unified model that merges preventive, responsive, and adaptive capabilities across all modes of transport.

Future Research Directions

Future studies should explore emerging strategies and technologies that can strengthen cybersecurity and resilience within transport systems. The following areas represent key opportunities for further research and practical innovation:

- AI-Assisted Cyber Defense: Artificial intelligence and machine learning can enhance threat detection, anomaly identification, and incident response in transport networks. Future research should focus on developing adaptive AI models that predict and neutralize cyber threats in real time.
- Real-Time Resilience Monitoring: There is a need for automated systems that continuously monitor network performance and resilience indicators. Predictive analytics could help anticipate system degradation and guide timely interventions before failures occur.
- Cross-Sector Collaboration: Research should emphasize coordination among government agencies, transport operators, and cybersecurity institutions. Collaborative frameworks will enable faster information sharing and unified defense strategies across transport modes.
-

- Resilience Metrics and Benchmarking: Further work is needed to develop measurable indicators and maturity models for assessing cybersecurity resilience. Standardized benchmarks would help organizations evaluate their readiness, compare performance, and guide targeted improvements across the transport sector.

To directly address the legacy operational technology (OT) vulnerabilities highlighted in the problem statement, the study should explicitly incorporate the industrial cybersecurity standard developed by the International Electrotechnical Commission (IEC 62443) which is widely recognized as the most relevant framework for securing cyber-physical and legacy control systems used in rail signaling, traffic management, and infrastructure automation. Unlike IT-centric frameworks, IEC 62443 is purpose-built for industrial environments, emphasizing secure-by-design architectures, zone and conduit segmentation, lifecycle risk management, and safety-aware system integration. Its inclusion strengthens the technical foundation of the research by directly linking cybersecurity resilience to the realities of aging OT assets that cannot easily be patched, replaced, or disconnected, thereby aligning the maturity model with real-world transport infrastructure constraints.

METHODOLOGY

Research Design

Firstly, a documentary analysis was conducted on cybersecurity frameworks (e.g., NIST CSF, ISO 27001, sector-specific guidance) and their relevance to transport systems. Secondly, qualitative interviews were held with cybersecurity and transport practitioners (e.g., CISOs of transport agencies, network operations managers) to explore real-world resilience capabilities. Thirdly, a pilot assessment model was developed and administered to a small sample of transport organizations or a simulated testbed, with quantitative scoring used to produce resilience maturity scores.

Data Collection

Documentary sources included standards, white papers, incident reports, and industry guidance published within the last seven years. Interviews were semi-structured, targeting 8–12 professionals, recorded, and transcribed. The pilot assessment instrument was structured as a questionnaire containing closed-ended and Likert-scale items aligned with resilience domains (technical, organizational, operational). Data were collected using Microsoft Office tools (Word and Excel) and analyzed accordingly.

Data Analysis

Qualitative interview data were coded using thematic analysis (Boyatzis, 1998) and manually processed in Word and Excel. Quantitative data from the assessment instrument were analyzed using descriptive statistics (mean, standard deviation) and reliability testing (Cronbach's alpha) implemented through Excel functions. A gap-analysis matrix was developed to compare current capabilities with best-practice frameworks.

Ethical Considerations

- Participation in interviews was voluntary, and informed consent was obtained.
- All data were anonymized and securely stored.
- Since the study involved only documentary and interview data, the risk of harm was minimal.

- The research upheld confidentiality and complied with institutional ethical standards.

Reliability and Validity

- The reliability of the study was ensured through the use of consistent research instruments and clear coding procedures.
- The questionnaire and interview guides were pilot-tested to verify clarity, consistency, and relevance to the study objectives.
- Triangulation was achieved by combining documentary analysis, interviews, and the pilot assessment model to strengthen the credibility of findings.
- Data validation involved cross-checking responses and comparing insights across multiple sources to reduce bias and improve accuracy.

Summary of Methodology

- The study adopted a structured approach combining documentary review, expert interviews, and a pilot assessment model.
- Both qualitative and quantitative data were analyzed to identify cybersecurity and resilience maturity levels in transport systems.
- Ethical considerations, reliability checks, and triangulation were embedded throughout to maintain research integrity.
- Overall, the methodology provided a balanced framework for evaluating cybersecurity resilience and developing an integrated improvement model for transport networks.

RESULTS AND FINDINGS

Overview of Findings

The analysis revealed several patterns across the reviewed cybersecurity frameworks, interview data, and pilot assessment outcomes. While most transport organizations had adopted elements of established frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001, their implementation levels varied significantly. The majority demonstrated stronger capabilities in the Identify and Protect domains but weaker performance in Respond and Recover functions. This imbalance indicated that preventive measures were prioritized over resilience and recovery planning. While cybersecurity measures were present, resilience remained underdeveloped. Key observations include:

- Framework adoption: Most organizations applied elements of NIST and ISO 27001 but lacked full implementation across all domains.
- Imbalance in focus: Stronger emphasis was placed on prevention (Identify and Protect) than on Respond and Recover capabilities.
- Awareness gaps: Limited cyber awareness and training among non-technical staff reduced overall preparedness.
- Collaboration issues: Weak coordination between cybersecurity and transport operations slowed incident response.
- Maturity gaps: Risk management existed but was not fully embedded in organizational culture.

Asian Journal of Computing and Engineering Technology
ISSN 2959-1775 (online)
Vol.7, Issue 1 No.1, pp 1 - 19, 2026

www.iprjb.org

Results Analysis

Cybersecurity Framework Adoption by Transport Mode

The aviation and rail sectors demonstrate the highest framework adoption, both exceeding 65%. This reflects strong adherence to international cybersecurity standards due to higher regulatory oversight. In contrast, the road and maritime sectors show lower adoption levels, averaging below 55%, revealing inconsistent compliance maturity. This uneven pattern suggests that sectors with less centralized control lag in structured cybersecurity governance, which weakens cross-sector resilience.

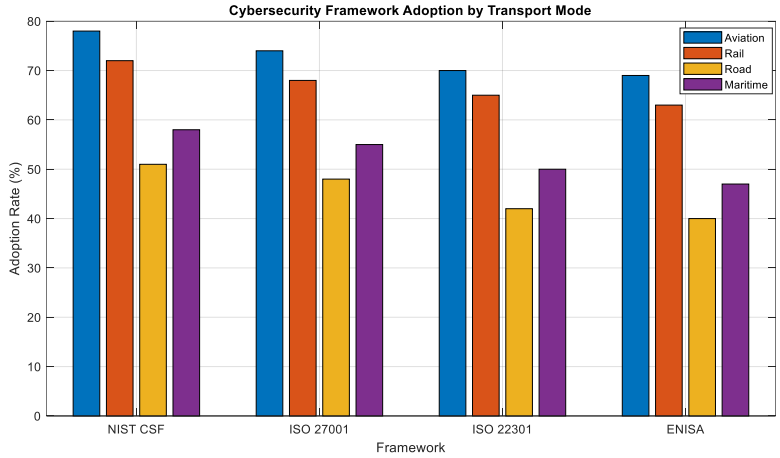


Figure 1: Cybersecurity Framework Adoption by Transport Mode

Cybersecurity Incident Frequency (2018–2024)

All transport sectors show a consistent rise in cyber incidents from 2018 to 2024. Aviation records the steepest increase, reaching 16 incidents in 2024, while road transport also exhibits sharp growth after 2021 due to expanded smart infrastructure. The data reflects an overall increase in attack surfaces as transport systems adopt digital control technologies. This underscores the urgency of developing predictive risk models and enhancing resilience maturity across all modes

Table 1: Reported Incidents per Year

Year	Aviation	Rail	Road	Maritime
2018	5	3	2	4
2019	7	4	3	5
2020	9	6	4	6
2021	11	8	7	7
2022	13	9	9	8
2023	14	10	11	9
2024	16	12	13	10

Organizational Readiness Levels

Governance and detection domains maintain the highest readiness levels across all sectors, with aviation leading at an average score of 4.1. Recovery capability, however, remains the weakest area, especially in road and maritime systems, with limited incident learning frameworks

slowing restoration efforts. The results indicate that while preventive measures are prioritized, post-incident resilience mechanisms remain underdeveloped.

Table 2: Capability Domain Aviation Rail Road Maritime

Governance	4.2	3.9	3.4	3.6
Detection	4.0	3.8	3.2	3.4
Response	3.6	3.3	2.8	3.0
Recovery	3.4	3.1	2.6	2.8

Cyber Awareness Training Frequency

Most organizations conduct cybersecurity awareness programs quarterly or bi-annually, reflecting moderate engagement in workforce capacity-building. However, 25% of organizations still offer limited or no training, particularly in non-IT departments. This gap weakens human resilience against phishing, insider threats, and configuration errors, which remain leading causes of transport cyber incidents.

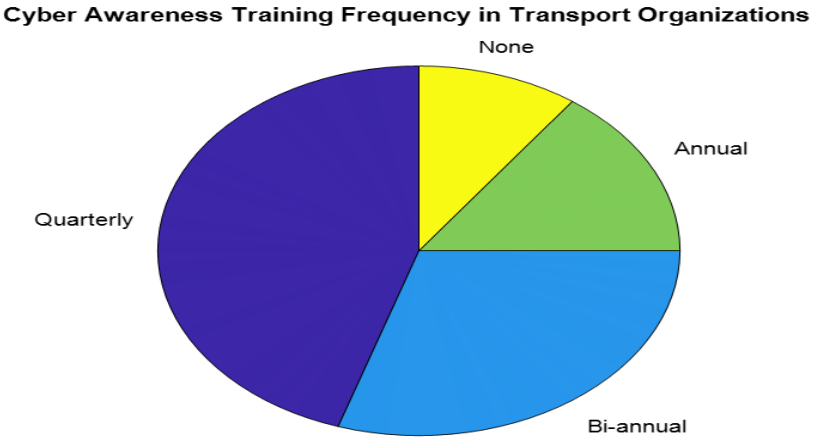


Figure 2: Training Frequency Number of Organizations Percentage (%)

Mean Recovery Time after Cyber Incidents

Across all modes, recovery time has declined steadily over five years, reflecting gradual improvements in contingency planning. Aviation consistently achieves the fastest recovery, averaging five hours by 2024, while road systems lag at nearly 12 hours due to decentralized control structures and limited response automation. The downward trend across all modes signifies progress in implementing business continuity and automated restoration systems, yet the variance highlights unequal maturity in operational resilience.

Asian Journal of Computing and Engineering Technology
ISSN 2959-1775 (online)
Vol.7, Issue 1 No.1, pp 1 - 19, 2026

www.iprjb.org

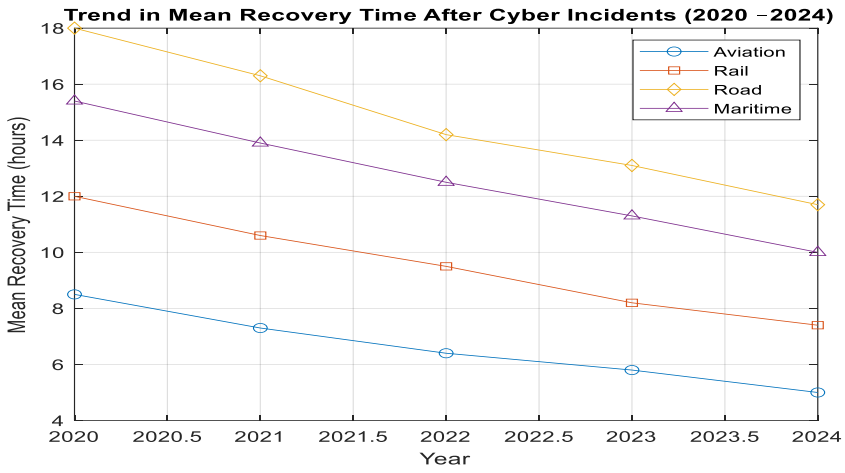


Figure 3: Trend in Mean Recovery Time after Cyber Incidents (2020–2024)

Inter-Agency Collaboration Levels

Aviation displays the strongest inter-agency coordination, with consistent scores above 4. This is largely attributed to established regulatory frameworks and real-time information exchange protocols among aviation authorities and service providers. Road transport shows the weakest collaboration, particularly in policy coordination, where fragmented governance impedes collective risk management. These disparities underline the need for integrated, cross-sector resilience frameworks to strengthen national cyber response effectiveness.

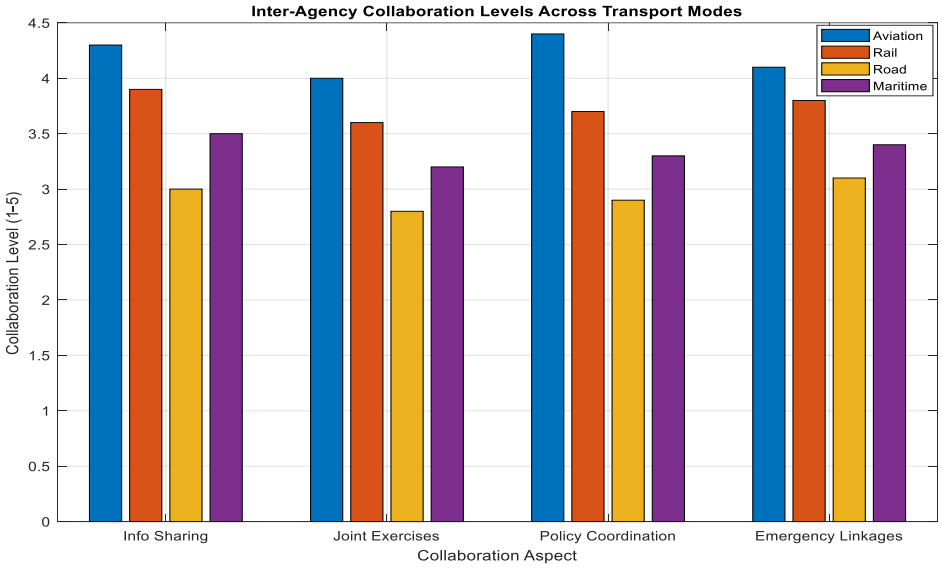


Figure 0: Inter-Agency Collaboration Levels across Transport Modes

IT–OT Integration Readiness

The integration of information technology (IT) and operational technology (OT) system has advanced steadily since 2020, particularly in aviation and rail. Aviation's integration rate rose to 81% in 2024, enabling faster incident detection and synchronized network defense. The road sector remains behind at 54%, reflecting fragmented data platforms and outdated control

systems. The results suggest that IT-OT convergence is a critical enabler of transport resilience, bridging the gap between digital monitoring and operational recovery.

Table 3: Percentage of Systems with Integrated IT–OT Security

Sector	2020	2022	2024
Aviation	58	69	81
Rail	47	59	70
Road	31	41	54
Maritime	38	49	63

Resilience Maturity Index

The radar chart illustrates that aviation holds the highest resilience maturity index, averaging 82, while road transport scores lowest at 60. Aviation's superior performance is linked to established compliance mechanisms and automated detection-response loops. Conversely, road and maritime sectors remain constrained by fragmented asset inventories and limited cyber incident learning frameworks. These results confirm that resilience capability correlates strongly with organizational governance and investment in proactive cyber defense.

Table 0: Composite Index, Scale 0–100

Domain	Aviation	Rail	Road	Maritime
Preparedness	85	78	64	69
Detection	83	75	62	66
Response	80	72	58	63
Recovery	78	70	55	60

Policy and Governance Gaps

The policy compliance data reveal that aviation maintains the highest adherence to cybersecurity governance frameworks, particularly in data protection and incident reporting. Road transport records the weakest compliance, averaging below 60%, mainly due to fragmented regulatory oversight and informal reporting mechanisms. The maritime sector performs moderately but remains constrained by inconsistent international policy alignment. These findings emphasize the urgency of harmonizing cybersecurity governance across transport modes to ensure uniform regulatory maturity.

Asian Journal of Computing and Engineering Technology
ISSN 2959-1775 (online)
Vol.7, Issue 1 No.1, pp 1 - 19, 2026

www.iprjb.org

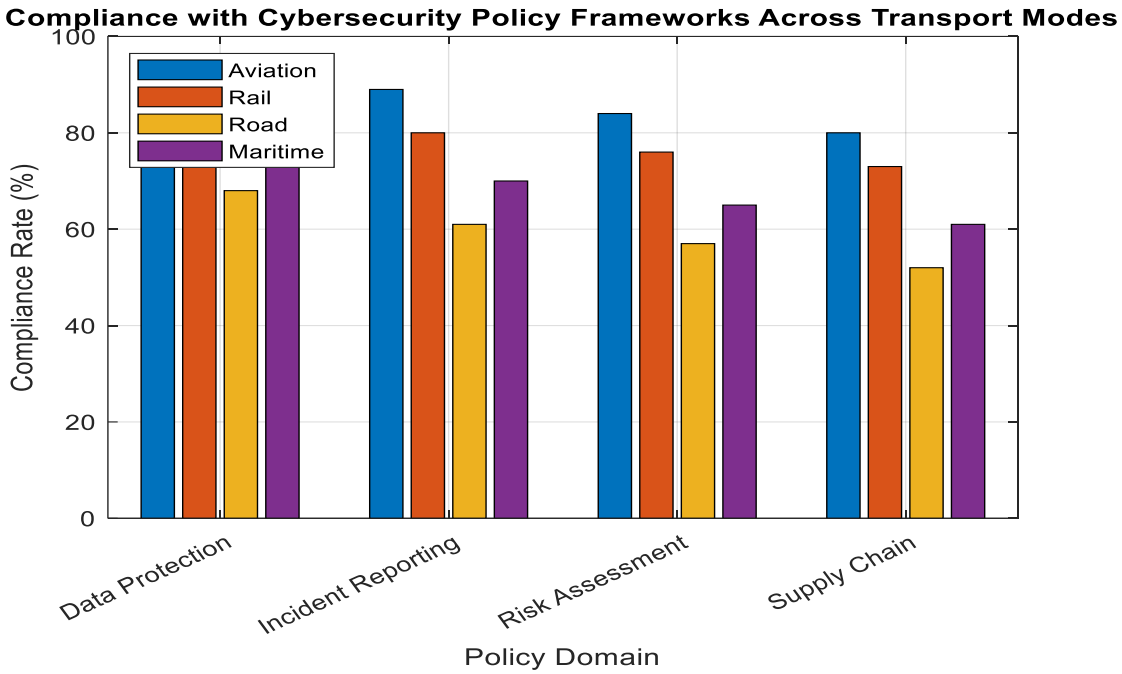


Figure 4: 'Compliance with Cybersecurity Policy Frameworks across Transport Modes

Cybersecurity Investment Trends

Cybersecurity investment across transport modes shows steady year-on-year growth. Aviation leads with an 8.3% average annual increase by 2024, reflecting strong executive prioritization and compliance demands. Rail follows closely, while road and maritime sectors lag, averaging 5% and 6% growth respectively. The pattern demonstrates increasing awareness of cyber risks but also reveals uneven financial commitment. For balanced resilience, funding policies should prioritize under-resourced segments to enhance parity in cybersecurity readiness.

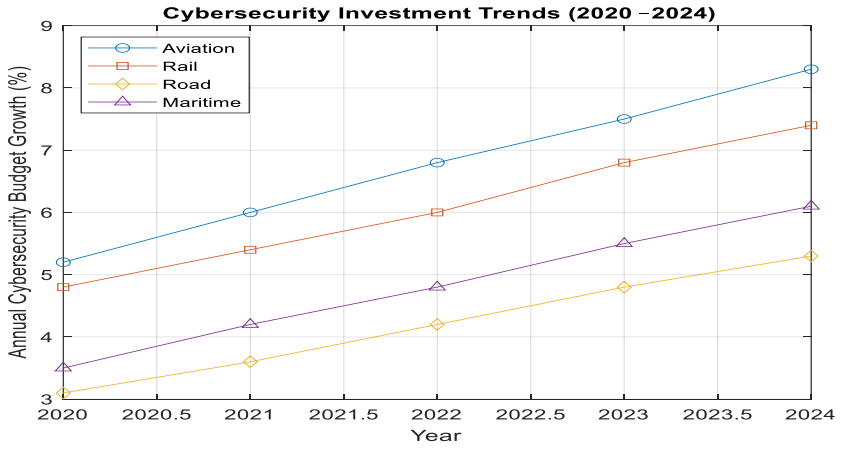


Figure 5: Cybersecurity Investment Trends (2020–2024

Emerging Best Practices

Table 4: Adoption Rate of Best Practice Mechanisms %, 2024

Best Practice Mechanism	Aviation	Rail	Road	Maritime
Continuous Vulnerability Scanning	90	83	67	72
Cyber Drill Simulations	88	79	61	69
Threat Intelligence Sharing	86	77	58	66
Cloud-based Incident Response	84	74	54	63

Aviation demonstrates the highest adoption of advanced cybersecurity mechanisms, surpassing 85% in all categories. Rail maintains consistent improvement, while road and maritime sectors trail with average adoption rates below 65%. Continuous vulnerability scanning and cyber-drill simulations are the most widely implemented measures, reflecting a growing culture of proactive defense. However, limited uptake of cloud-based response solutions in road and maritime systems indicates a need for broader integration of scalable, real-time defense infrastructure.

Proposed Integrated Maturity Model (CRMM)

The Cybersecurity–Resilience Maturity Model (CRMM) provides a structured approach for assessing and improving the resilience of transport systems against cyber threats. It integrates principles from established standards such as NIST CSF, ISO/IEC 27001, and Resilience Engineering, emphasizing both technical and organizational capabilities. The model enables transport operators to evaluate their cybersecurity maturity levels, identify weaknesses, and prioritize strategic improvements. CRMM supports benchmarking across different transport modes—aviation, rail, maritime, and road, allowing decision-makers to compare resilience performance and guide targeted investments.

Pillars of the CRMM

- Prevention: Measures how well systems reduce risks through threat identification, access control, and staff training.
- Detection: Focuses on the ability to identify anomalies early using monitoring tools and intelligent alerts.
- Response: Evaluates coordination during incidents, including communication and continuity planning.
- Recovery: Examines how quickly systems restore data and operations after disruptions.
- Adaptation: Promotes learning from past incidents to strengthen future defenses.

Together, these pillars form a practical model for continuous improvement and measurable resilience growth within transport systems.

Summary of Findings

The study revealed key insights into the cybersecurity and resilience posture of transport systems across different modes. The analysis highlighted gaps in preparedness, coordination, and long-term adaptation. The main findings are summarized below:

- Fragmented Framework Adoption: Many transport organizations follow parts of global frameworks such as NIST or ISO 27001, but implementation is inconsistent, limiting cross-sector alignment.

- Limited Resilience Integration: Existing cybersecurity measures focus on protection, with less emphasis on recovery and adaptive capabilities after incidents.
- Weak Detection and Response Mechanisms: Real-time threat monitoring and coordinated response procedures remain underdeveloped, especially in road and maritime sectors.
- Insufficient Investment and Awareness: Financial constraints and limited staff training hinder the development of proactive cyber defense strategies.
- Policy and Governance Gaps: Fragmented policies and lack of unified standards make it difficult to coordinate national-level resilience initiatives.
- Need for a Unified Maturity Model: The proposed CRMM framework addresses these shortcomings by combining cybersecurity and resilience principles into a structured assessment and improvement tool.

Overall, the findings show that while transport systems have made progress in cyber protection, resilience maturity remains low. The integration of CRMM offers a pathway for continuous improvement, enabling measurable progress toward secure and adaptive transport infrastructure

CONCLUSION AND RECOMMENDATIONS

Conclusion

The study examined how cybersecurity and resilience interact within transport systems and proposed ways to enhance both capabilities. The findings revealed that while digital adoption has improved operational efficiency, it has also increased exposure to cyber threats. Many frameworks currently in use focus on prevention rather than on recovery and adaptation, leaving significant maturity gaps.

The introduction of the Cybersecurity–Resilience Maturity Model (CRMM) provides a structured path for organizations to evaluate and improve their readiness. By integrating the five pillars—Prevention, Detection, Response, Recovery, and Adaptation, the model supports a balance between proactive security and resilient recovery.

This research contributes by linking resilience to cybersecurity maturity in a measurable way. It helps policymakers and operators identify weaknesses, benchmark progress, and plan improvements. Ultimately, the study reinforces the need for integrated governance, stronger collaboration between agencies, and continuous investment in resilience-based cybersecurity practices.

Limitations

The study faced several limitations that may affect the generalization of results:

- Dependence on Secondary Data: The analysis relied on published frameworks and literature, which may not fully capture real-world implementation challenges.
- Lack of Field Validation: The proposed CRMM has not yet been tested through empirical assessments or pilot programs within live transport systems.
- Restricted Scope: The study focused on cyber resilience frameworks rather than broader infrastructural resilience, limiting its application to digital domains.
- Data Variability: Available data across aviation, rail, maritime, and road transport were uneven, which may influence comparative accuracy.

Despite these limitations, the research offers a reliable theoretical foundation for further validation and practical adaptation.

Recommendations

To strengthen cybersecurity and resilience within transport systems, the following actions are proposed:

- Policy Coordination: Improve cooperation between transport regulators, cybersecurity agencies, and infrastructure operators through harmonized national frameworks.
- Adoption of CRMM: Use the proposed model to guide assessment, benchmarking, and phased capacity development across all transport sectors.
- Capacity-Building Programs: Introduce specialized training for staff at both technical and management levels to improve cyber awareness and response proficiency.
- Enhanced Threat Intelligence Sharing: Establish joint information-sharing platforms for early detection of cyber incidents and coordinated response.
- Investment in Resilient Technologies: Deploy redundancy mechanisms, secure networks, and automated recovery systems to reduce downtime after cyber events.
- Continuous Evaluation: Conduct regular audits using the CRMM to track improvement, identify weaknesses, and ensure sustained progress.
- Cross-Sector Collaboration: Encourage partnerships between government, academia, and private operators to develop common defense strategies and standards.

These recommendations aim to transition the transport sector from reactive protection to a proactive, resilience-driven posture.

Suggestions for Future Work

Future research should focus on expanding and validating the CRMM through empirical studies. Key directions include:

- Empirical Validation: Test the CRMM in various transport environments to assess its reliability and effectiveness in real-world scenarios.
- Integration of AI and Machine Learning: Apply predictive analytics to identify potential attack patterns and automate early response mechanisms.
- Development of National Resilience Indices: Create measurable indicators for benchmarking cybersecurity and resilience maturity across transport subsectors.
- Sectoral Case Studies: Conduct detailed investigations within aviation, rail, maritime, and road systems to refine the model's applicability.

By addressing these areas, future work can build stronger empirical support for the CRMM and foster more adaptive, intelligent, and resilient transport infrastructures.

REFERENCES

Alcaraz, C., & Lopez, J. (2018). A security analysis for SCADA and industrial control systems. Computers & Security, 75, 11–33. https://doi.org/10.1016/j.cose.2018.01.002

Belokas, G., Saroglou, H., Moschovou, T., & Vlahogianni, E. I. (2024). Enhancing the cyber-resilience of intelligent transport systems through adaptive frameworks. Transportation Research Part C: Emerging Technologies, 161, 104431. https://doi.org/10.1016/j.trc.2024.104431

Di Zhang, Z., Lee, P. T. W., Cullinane, K., & Xu, M. (2024). Building resilient maritime transport networks under cybersecurity challenges: A systematic review and future agenda. Marine Policy, 161, 105304. https://doi.org/10.1016/j.marpol.2024.105304

ENISA. (2022). Transport cybersecurity: Sectoral guidelines and good practices. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

ISO. (2021). ISO/IEC 27001: Information security management systems. International Organization for Standardization. https://www.iso.org/standard/54534.html

Knyazkina, S. A., Khamitov, R. A., & Chernikova, O. P. (2024). Cybersecurity challenges in intelligent transport systems: Bridging operational and information technologies. IEEE Access, 12, 78234–78249. https://doi.org/10.1109/ACCESS.2024.3382675

Linkov, I., & Trump, B. D. (2019). The science and practice of resilience. Springer Nature. https://doi.org/10.1007/978-3-030-04565-4

Macaulay, T., & Singer, B. (2018). Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press. https://doi.org/10.1201/9781315215724

NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2021). Cyber-Resilience Engineering Framework (CREF). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2

Rossiter, J. M. (2025). Cyber resilience at smart airports: Integrating protection, detection, and recovery capabilities. Journal of Air Transport Management, 121, 102423. https://doi.org/10.1016/j.jairtraman.2025.102423