

Cybersecurity Digital Solutions in Railway Applications: Architecture, Standards, and Next-Generation Defenses

The Imperative for Cyber-Physical Security in Modern Rail

The railway sector is undergoing a profound structural evolution, shifting from isolated, electromechanical signaling paradigms to highly interconnected, cyber-physical ecosystems. Historically, railway operations relied on physical airgaps and closed-loop proprietary protocols to maintain functional safety. However, the modernization of railway networks—driven by demands for higher capacity, interoperability, and automated train operations (ATO)—has effectively dissolved these perimeters. Modern trains operate as high-speed data centers, exchanging continuous telemetry with trackside object controllers, regional traffic management systems (TMS), and cloud-hosted analytics platforms¹.

This hyper-connectivity has fundamentally altered the industry's risk profile. The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2025 report analyzed over 4,875 incidents, identifying the transport sector as the second most targeted industry in the European Union⁴. The threat actors targeting these systems have matured from financially motivated cybercriminals deploying generic ransomware to sophisticated hacktivists and state-aligned Advanced Persistent Threats (APTs) seeking to disrupt critical national infrastructure (CNI)⁷.

The consequences of a successful cyber-physical intrusion extend far beyond data loss; they present direct, kinetic threats to human life and economic stability⁹. In 2021, an attack attributed to state-aligned actors disrupted the Iranian railway network, hijacking station display boards to broadcast fraudulent delay messages while simultaneously deploying wiper malware to cripple operational technology (OT) systems¹⁰. Similar methodologies, including the exploitation of Windows BitLocker bypasses and exposed API keys, have been observed in state-sponsored campaigns against Albanian government infrastructure and broader logistics networks, underscoring the geopolitical leverage inherent in transport disruption¹⁰.

Protecting these environments requires a holistic architectural strategy. The defense mechanisms must account for the intersection of dynamic cybersecurity requirements and stringent functional safety certifications, the harmonization of global regulatory standards, and the deployment of advanced digital solutions tailored to the unique operational realities of the railway domain⁹.

Vulnerabilities in Railway Communication Architectures

Railway communications are highly specialized, generally categorized into train-to-ground (T2G) signaling networks, intra-consist Train Communication Networks (TCN), and decentralized field control architectures. Each layer was originally designed with an implicit assumption of physical security, resulting in structural vulnerabilities that modern threat actors are increasingly equipped to exploit.

Train-to-Ground Signaling: GSM-R, ERTMS, and the FRMCS Transition

The European Rail Traffic Management System (ERTMS) relies on the European Train Control System (ETCS) to dictate train movements. ETCS utilizes the Global System for Mobile Communications-Railway (GSM-R) to facilitate continuous two-way communication between the onboard European Vital Computer (EVC) and the trackside Radio Block Centre (RBC)¹⁴. The security of this signaling layer is governed by the EuroRadio protocol, which provides authentication for the train control application¹⁶.

However, cryptographic analyses of ERTMS baselines have exposed severe vulnerabilities within this stack. The current standards rely heavily on deprecated cryptographic primitives, specifically Triple DES (3DES), to generate Message Authentication Codes (MACs)¹⁶.

Researchers have successfully demonstrated collision attacks against EuroRadio. When combined with application-level design flaws, an adversary capturing a MAC collision can forge train control messages or execute session hijacking, potentially feeding false movement authorities to the EVC¹⁶. Furthermore, physical trackside assets such as Eurobalises, which transmit critical localization data to passing trains, often lack robust integrity protection or dynamic authentication. This exposes them to localized spoofing, radio jamming, and malicious data injection using low-cost software-defined radios¹⁷.

To mitigate these vulnerabilities, the railway industry is migrating to the Future Railway Mobile Communication System (FRMCS), leveraging 4G and 5G cellular architectures³. While FRMCS resolves the cryptographic weaknesses of GSM-R by utilizing the inherently stronger security of modern cellular networks, it shifts the attack surface to the service and application layers. Security models evaluating FRMCS at level crossings have identified new threat vectors, including sophisticated functional identity takeovers, volumetric Denial of Service (DoS) attacks, and the abuse of railway emergency call functions⁹.

Intra-Consist Networks: TRDP and Multicast Vulnerabilities

Within the rolling stock, the Train Communication Network (TCN), governed by the IEC 61375 standard, manages data exchange between critical vehicle subsystems such as propulsion, braking, and passenger information systems¹⁸. The Train Real-time Data Protocol (TRDP) serves as the backbone for the Ethernet Consist Network (ECN), engineered to provide deterministic, low-latency communication²².

TRDP achieves its necessary speed by utilizing multicast communication profiles, broadcasting

process data to multiple onboard subsystems simultaneously²³. Because multicast is a one-to-many architecture, establishing traditional point-to-point cryptographic tunnels, such as Transport Layer Security (TLS), is computationally prohibitive and introduces latency that violates the strict timing requirements of train control²³. Consequently, raw TRDP traffic is vulnerable to packet sniffing, replay attacks, and malicious message injection¹⁸. The industry is responding by developing lightweight, message-oriented security layers, such as SecDT, for TRDP communications. SecDT introduces configurable cryptographic profiles that provide message authentication and integrity without significantly penalizing data delivery latency²³. Unlike IoT protocols such as MQTT, which rely on a centralized broker that introduces a single point of failure and additional latency, SecDT operates natively within the multicast environment and ensures backward compatibility, allowing non-secure devices to continue functioning on segregated communication IDs²³.

Field Control Interoperability: EULYNX and RaSTA

On the trackside, infrastructure managers are moving away from proprietary, monolithic signaling systems toward modular, standardized architectures driven by the EULYNX consortium²⁵. EULYNX separates the central interlocking logic from the physical trackside elements (such as points, signals, and level crossings) through the use of decentralized Object Controllers (OCS)²⁷.

The communication between the central safety logic and the OCS relies on Standardized Control Interfaces (SCI) and Standardized Diagnostic Interfaces (SDI), utilizing the Rail Safe Transport Application (RaSTA) protocol²⁷. RaSTA was designed to ensure functional safety by mitigating transmission errors like repetition, deletion, and sequence corruption²⁹. To secure these links against cyber threats, EULYNX specifies that RaSTA traffic must be encapsulated within TLS over TCP²⁹.

While this encapsulation provides robust confidentiality and integrity, achieving Security Level 3 (SL3) compliance across thousands of distributed wayside cabinets introduces immense operational complexity. It necessitates a highly available Public Key Infrastructure (PKI) to manage certificate lifecycles, endpoint authentication, and secure key exchanges without compromising operational continuity or causing signaling latency²⁷. Projects such as Digirail in Finland demonstrate the practical implementation of this architecture, utilizing Mipro Object Controller Systems to blend SIL 4 functional safety with EULYNX-compliant, TLS-encrypted cybersecurity²⁸.

Network Segment	Primary Protocols	Core Vulnerabilities	Modern Mitigation Architectures
Train-to-Ground	GSM-R, EuroRadio	3DES weaknesses, MAC collisions,	Migration to FRMCS (5G),

(Signaling)		Eurobalise spoofing and jamming ¹⁶ .	implementation of Post-Quantum Cryptography (PQC) ⁹ .
Intra-Consist (Onboard)	IEC 61375, TRDP, MVB	Multicast traffic lacks native encryption; susceptible to injection and replay ¹⁸ .	Deployment of lightweight SecDT profiles, network segmentation, deep packet inspection ²³ .
Field Control (Trackside)	EULYNX SCI, RaSTA	Physical access to wayside cabinets, unauthorized diagnostic polling ²⁸ .	RaSTA encapsulation in TLS/TCP, strict PKI certificate lifecycle management ²⁸ .

The Convergence and Conflict of Safety and Security

In the railway domain, cybersecurity is irrevocably tied to functional safety. The industry has long relied on the CENELEC RAMS framework—specifically EN 50126 (Process), EN 50128 (Software), and EN 50129 (System Safety)—to dictate the rigorous certification procedures required for any safety-critical electronic system³³.

This regulatory environment creates a profound operational conflict between traditional IT cybersecurity practices and railway safety engineering. In conventional IT, the discovery of a critical zero-day vulnerability prompts immediate patching and system reboots. However, under EN 50129, modifying the software, firmware, or configuration of a safety-certified system (such as an interlocking controller or an automatic train protection module) risks voiding its safety case⁹. If a security patch introduces a minor software bug that delays a braking command by mere milliseconds, the cyber mitigation itself transforms into a kinetic safety hazard³⁵.

Consequently, the railway industry has adopted integrated safety-security co-engineering paradigms. The UK Department for Transport and the Claims, Argument, Evidence (CAE) framework assert that claims regarding system safety must be informed by security considerations, acknowledging that unmitigated cyber vulnerabilities inherently contravene regulatory safety requirements¹³. To resolve the patching conflict, engineers increasingly rely on defense-in-depth and compensating controls. By placing passive network intrusion detection systems and strict access control gateways in front of legacy controllers, infrastructure managers can isolate the vulnerability at the network perimeter. This allows the safety-certified endpoint to remain logically and physically unaltered, preserving the EN 50129

safety case while successfully mitigating the cyber risk³⁵.

Harmonization of International Cybersecurity Standards

To systematically address the intersection of safety and security, the global railway ecosystem is harmonizing around structured risk assessment frameworks, translating broad industrial guidelines into actionable railway engineering practices.

IEC 62443 and the Zones and Conduits Methodology

The cornerstone of modern operational technology security is the ISA/IEC 62443 series. Central to this standard is IEC 62443-3-2, which mandates the partitioning of Industrial Automation and Control Systems (IACS) into Zones and Conduits³⁸. A zone is defined as a logical grouping of physical and functional assets that share similar security requirements (e.g., a "Rolling Stock Control Zone" or a "Station Enterprise IT Zone"). A conduit represents the specific communication pathway facilitating data flow between these zones³⁹.

Implementing IEC 62443-3-2 in a railway environment follows a precise Zonal Cyber Risk (ZCR) workflow⁴⁰:

1. **ZCR 1 & 2 (Initial Assessment):** The organization defines the System Under Consideration (SuC) and conducts a high-level risk assessment to determine the worst-case, unmitigated impact of a breach on functional safety and operational availability³⁸.
2. **ZCR 3 (Partitioning):** The SuC is divided into zones and conduits. Network devices, such as firewalls and data diodes that enforce the conduits, are placed into distinct configuration zones managed exclusively by OT security specialists, ensuring that corporate IT cannot inadvertently compromise safety-critical routing³⁹.
3. **ZCR 4 & 5 (Detailed Assessment and Target Levels):** Engineers identify specific threat scenarios and system vulnerabilities, assessing the likelihood and impact. Based on this, a Security Level Target (SL-T) is assigned to each zone, ranging from SL 1 (protection against casual or coincidental violation) to SL 4 (protection against highly resourced, state-sponsored attacks)⁴⁰.
4. **ZCR 6 & 7 (Requirements and Approval):** Cybersecurity requirements are documented based on the SL-T, and the formal risk decisions are presented to the asset owner for binding organizational approval⁴¹.

CLC/TS 50701 and the Development of IEC 63452

Recognizing that the horizontal IEC 62443 standard lacked the nuances required for distributed, mobile railway infrastructure, the European Committee for Electrotechnical Standardization (CENELEC) published the technical specification CLC/TS 50701 in 2021⁴². TS 50701 contextualizes the IEC 62443 framework explicitly for the railway domain, aligning cybersecurity risk assessments seamlessly with the EN 50126 RAMS lifecycle⁴³.

Because TS 50701 operates as a European technical specification, there is an industry-wide

imperative to elevate it to a fully international standard. The International Electrotechnical Commission (IEC) established Project Team (PT) 63452 to execute this transition. The forthcoming IEC 63452 standard expands upon TS 50701 by formalizing normative clauses for cybersecurity acceptance, enhancing threat intelligence integrations, and providing comprehensive operational and decommissioning requirements⁴². The standard has progressed rapidly, with a Committee Draft for Vote (CDV) targeted for late 2024 and final publication as an International Standard expected by July 2025⁸.

Interoperability and Regulatory Frameworks

Beyond voluntary standards, stringent regulatory mandates are reshaping railway compliance. The European Union's NIS2 Directive categorizes major transport operators as essential entities, enforcing strict policies on risk analysis, incident reporting, and supply chain security⁴⁵. Concurrently, the Cyber Resilience Act (CRA) places legal obligations on railway Original Equipment Manufacturers (OEMs) to ensure their products are secure by design throughout their lifecycle⁴⁷.

At the network level, the Control-Command and Signalling Technical Specification for Interoperability (TSI CCS 2023) dictates the mandatory requirements for ERTMS and GSM-R across the European rail network³⁴. The TSI CCS explicitly mandates cybersecurity risk-management measures, requiring infrastructure managers to manage cryptographic keys and authenticate communication channels in strict accordance with the baseline specifications (such as ETCS BL4 and FRMCS BLO)³⁴.

Regulatory / Standard Framework	Primary Focus / Domain	Key Impact on Railway Cybersecurity
EN 50126 / 50128 / 50129	RAMS & Functional Safety	Establishes the safety case; restricts ad-hoc software patching to prevent kinetic hazards ³³ .
IEC 62443-3-2	Industrial OT Security	Dictates the partitioning of systems into Zones and Conduits; establishes Security Level Targets (SL-T) ³⁸ .
CLC/TS 50701	Rail-Specific Cyber Specification	Bridges IEC 62443 with EN 50126, translating generic IT/OT concepts into specific

		rolling stock and signaling models ⁴² .
IEC 63452 (Upcoming)	International Rail Cyber Standard	Elevates TS 50701 to a global normative standard, expected in 2025, facilitating verifiable certification ⁸ .
TSI CCS 2023	European Interoperability	Enforces mandatory ERTMS baselines and cryptographic key management for cross-border rail traffic ³⁴ .

Regional Mandates: Securing National Infrastructure

While European standards drive much of the global engineering consensus, regions outside of Europe are implementing highly customized, stringent regulatory frameworks to protect their specific geopolitical and economic interests.

Saudi Arabia: The NCA Regulatory Ecosystem

In the Kingdom of Saudi Arabia, the rapid modernization of infrastructure under Vision 2030 has necessitated an aggressive cybersecurity posture, directed by the National Cybersecurity Authority (NCA)⁵⁰. The NCA enforces compliance through several rigorous, mandatory frameworks that deeply impact entities like the Saudi Railway Company (SAR), which manages extensive freight and high-speed passenger networks⁵⁰.

The Essential Cybersecurity Controls (ECC-2:2024) form the baseline, mandating continuous risk management, rigorous third-party vendor assessments, and the compulsory use of Multi-Factor Authentication (MFA) across all remote access and administrative connections⁵². However, because the railway sector is classified as critical infrastructure, operators must adhere to the more stringent Critical Systems Cybersecurity Controls (CSCC-1:2019)⁵⁴.

The CSCC elevates cybersecurity to a matter of national defense. It explicitly mandates physical and logical network segmentation, requires quarterly disaster recovery testing, and imposes strict data sovereignty laws⁵⁴. Under the CSCC, critical systems must be hosted within the Kingdom; remote access from outside Saudi Arabia is heavily restricted or prohibited, and any outsourced cybersecurity monitoring or managed services must be conducted by vendors physically located within the nation⁵³. Furthermore, the Operational Technology Cybersecurity Controls (OTCC-1:2022) align NCA mandates with IEC 62443 principles, providing a specialized mapping guide to ensure that zero-trust architectures and continuous monitoring are effectively deployed across traction power substations and traffic control centers without

disrupting operations⁵⁵.

Jordan: The NCSC and the Aqaba Railway Corporation

The Hashemite Kingdom of Jordan similarly recognizes the transportation sector as vital to its national security and economic reputation. Operating under Cybersecurity Law No. 16 of 2019, the National Cyber Security Center (NCSC) explicitly designates government services and transportation as critical national infrastructure⁵⁷.

The NCSC enforces the Jordan National Cybersecurity Framework (JNCSF), requiring infrastructure operators to adhere to 12 foundational domains, including strict access control, incident response, and continuous network monitoring, assessed via the Jordan Cybersecurity Compliance Tool (JCCT)⁵⁸. This framework is highly relevant to the Kingdom's strategic logistics initiatives, most notably the operations of the Aqaba Railway Corporation (ARC). Historically focused on phosphate transport, the ARC is central to the "Jordan National Railway Network Project," a massive undertaking aimed at linking Aqaba with Amman and regional borders⁶⁰. As these freight networks undergo digital transformation and integrate modern signaling technologies, strict compliance with the JNCSF is mandatory to protect the logistics backbone from regional cyber disruptions and ensure operational continuity⁵⁸.

Commercial Ecosystem and Market Solutions

The complex demands of railway cybersecurity—navigating proprietary protocols, stringent safety regulations, and zero-latency operational requirements—have cultivated a highly specialized commercial ecosystem. The market is defined by pure-play rail security startups, massive rolling stock original equipment manufacturers (OEMs), and broad industrial OT platforms³⁶.

Rail-Specific Security Pioneers

A new vanguard of companies focuses exclusively on the unique architectures of ERTMS, CBTC, and TCN networks, providing solutions that general IT firewalls cannot replicate.

- **Cylus:** Headquartered in Israel, Cylus developed the *CylusOne* platform, explicitly designed to parse rail protocols without inducing latency. The platform provides continuous asset visibility, behavioral anomaly detection, and vulnerability management mapped directly to the physical rail topology³⁶.
- **RazorSecure:** A UK-based specialist focused deeply on rolling stock security and compliance with TS 50701 and the CRA. RazorSecure provides solutions like *Delta* for onboard intrusion detection and Secure Digital Maintenance Gateways to strictly control third-party access to train networks, ensuring configuration drift is immediately identified⁴⁸.
- **Cervello:** Another leading Israeli firm providing rail-specific passive monitoring, threat intelligence, and analytics platforms, heavily utilized by urban metro operators to secure complex wayside and onboard infrastructures⁶⁶.
- **Orbik Cybersecurity:** Specializing in the engineering lifecycle, Orbik assists rail manufacturers in designing compliant products that meet IEC 62443 and Cyber

Resilience Act standards from the conceptual phase through to deployment³⁶.

OEM Integration and Strategic Partnerships

The companies that physically build the trains and signaling infrastructure have recognized that cybersecurity is a fundamental prerequisite for winning modern tenders.

- **Alstom:** As a global mobility leader, Alstom has internalized cybersecurity, deploying over 420 rail-focused security specialists. To accelerate their capabilities, Alstom invested \$7 million in 2020 to acquire a minority stake in Cylus². This partnership integrates Cylus's advanced threat detection natively into Alstom's CBTC and ETCS solutions, with early deployments on the Tel Aviv Red Line⁶⁴. Furthermore, Alstom partners with Airbus Protect for risk assessment tools, Capgemini for Security Operations Center (SOC) monitoring, and academic institutions like the Rochester Institute of Technology (RIT) to cultivate the next generation of rail cybersecurity engineers².
- **Thales and Hitachi Rail:** These major integrators build security directly into their hardware, offering robust cryptography, secure signaling architectures (such as SelTrac), and comprehensive consulting services tailored to national mass transit networks³⁶.

Industrial OT Security Platforms

Broad industrial security leaders such as Claroty, Nozomi Networks, and Dragos also support the rail ecosystem. While not exclusively focused on rail protocols, their Deep Packet Inspection (DPI) and passive anomaly detection frameworks are highly effective at securing the broader operational environment, including traction power substations, station HVAC systems, and the underlying ethernet networks that support the railway infrastructure³⁶.

Next-Generation Digital Solutions for Rail

Cybersecurity

To protect both legacy brownfield systems and modern greenfield deployments while adhering to the rigorous standards of IEC 62443 and TS 50701, the industry is adopting a targeted suite of next-generation digital solutions. Based on extensive sector analysis and collaborative workshop outputs, the following digital architectures represent the forefront of railway cyber defense³⁶.

Protocol-Aware AI Signalling Sentinels (Passive IDS)

Standard enterprise firewalls are blind to the syntax of proprietary interlocking telegrams or ERTMS/ETCS communications. To achieve the continuous monitoring required by IEC 62443-3-3 (Timely Response to Security Events), operators deploy Protocol-Aware AI Signalling Sentinels. These passive, non-invasive Intrusion Detection Systems (IDS) utilize zero-latency mirroring architectures, ensuring that the RAMS safety certification is never compromised. By applying neural network models to baseline normal telegram exchanges between the RBC and trackside elements, the Sentinel instantly detects anomalous message injection, packet replay attacks, or abnormal polling rates characteristic of advanced state-actor reconnaissance³⁶.

AI-Powered USB Inspection and Sanitization Gateways

A critical vulnerability in legacy rail environments is the "sneakernet"—field engineers inserting unmanaged USB drives or connecting diagnostic laptops directly into airgapped trackside cabinets³⁶. To fulfill IEC 62443-3-3 requirements concerning Portable Media Control and Restricted Data Flow, operators utilize ruggedized hardware-software kiosks deployed at maintenance depots. Before any media is permitted to interface with a legacy controller, the AI-kiosk utilizes machine learning to sandbox and scan firmware updates, configuration files, and diagnostic scripts for hidden malware or unauthorized code. Only after cryptographic verification is the USB cleared for use, eliminating unmonitored human workarounds³⁶.

Secure Digital Maintenance Gateways (SDMG)

Managing remote access for third-party vendors and field engineers requires strict adherence to Zero-Trust Architecture. The Secure Digital Maintenance Gateway (SDMG) replaces traditional, persistent VPN connections with a time-bound, encrypted proxy tunnel. The SDMG enforces multi-factor authentication (MFA) and performs automated command-line logging for every action executed on remote interlocking huts or traction substations. Once the associated maintenance ticket is closed, access privileges are automatically revoked, drastically reducing the attack surface exposed by compromised vendor credentials³⁶.

On-Board Rolling Stock Asset and Vulnerability Profilers

Modern rolling stock contains highly complex internal networks, including MVB, CAN, and Ethernet (TRDP). Continuous inventory tracking is essential for maintaining compliance with CLC/TS 50701. On-board asset profilers dynamically discover hardware and software inventories across the moving consist, monitoring firmware changes and detecting unauthorized plug-in devices. By correlating this real-time inventory against known CVE (Common Vulnerabilities and Exposures) databases, operators can accurately assess their risk posture and prioritize patching strategies during scheduled depot maintenance³⁶.

Digital Twin Attack Simulation and Resiliency Engines

Because active penetration testing cannot be safely conducted on live, safety-critical railway systems, the industry is turning to Digital Twins. A cloud-connected virtual simulation environment perfectly models the railway's specific signaling logic, EULYNX interface topologies, and physical track layout³⁶. This supports IEC 62443-2-4 requirements by providing a safe sandbox where security teams can run automated red-teaming scripts. Engineers can simulate DoS attacks, data spoofing, and cascading equipment failures to measure system recovery times, test redundancy thresholds, and validate the resilience of the network architecture before any physical deployment occurs³⁶.

IEC 62443-Aligned Field Assessment and Compliance Platforms

Gathering accurate physical security data from remote trackside locations requires purpose-built tools. Field Assessment and Compliance Platforms provide tablet-optimized, offline-first auditing applications for signaling maintenance crews. As technicians inspect remote interlocking huts, they log physical security postures, asset configurations, and

environmental conditions. The platform automatically maps these field observations against IEC 62443 Security Levels (SL 1–4) and TS 50701 risk assessment methodologies, instantly generating compliance gap reports and remediation workflows for centralized management dashboards³⁶.

Encrypted Hybrid Cloud Resiliency Meshes and Post-Quantum Preparation

As traffic management systems migrate to the cloud, maintaining strict segmentation between enterprise IT layers and critical OT is paramount. The Encrypted Hybrid Cloud Resiliency Mesh represents a zero-trust cloud-edge architecture. It utilizes hardware-enforced data diodes and encrypted VPN tunnels to ensure that heavy data analytics occur in the cloud, while safety-critical interlocking decisions remain strictly localized at the edge³⁶. Furthermore, recognizing the long lifecycles of rail assets, this architecture prepares the infrastructure for Post-Quantum Cryptography (PQC) standards. By implementing agile cryptographic key management systems now, operators ensure that their communication channels will remain secure against the advanced computational attacks anticipated in the coming decades³¹.

Strategic Synthesis and Future Outlook

The transition of the railway sector into a fully digitized, cyber-physical ecosystem has irrevocably bound functional safety to cybersecurity. The historical reliance on closed, proprietary networks and physical airgaps has been rendered obsolete by the integration of ERTMS, EULYNX standardizations, FRMCS 5G deployments, and cloud-hosted traffic management. As geopolitical tensions rise and state-sponsored actors increasingly target transportation networks for maximum disruptive impact, the implementation of robust, defense-in-depth strategies is an absolute operational necessity.

Navigating this transition requires strict adherence to harmonized international frameworks. The evolution of CLC/TS 50701 into the normative IEC 63452 standard provides the railway ecosystem with a definitive, lifecycle-based blueprint for assessing zonal risks and implementing appropriate Security Level Targets. Simultaneously, regulatory mandates—such as the Saudi NCA controls, the Jordanian JNCSE, and the European NIS2 and CRA directives—are enforcing structural accountability, demanding that cybersecurity be integrated natively into product design and operational maintenance.

To meet these rigorous demands without invalidating existing EN 50129 safety certifications, railway operators and OEMs are heavily leveraging specialized commercial partnerships and advanced digital solutions. By deploying protocol-aware AI intrusion detection systems, enforcing zero-trust maintenance gateways, sanitizing physical media at the edge, and utilizing digital twins for risk simulation, the industry can bridge the gap between static safety engineering and dynamic cyber defense. Ultimately, the successful deployment of these architectures ensures that the next generation of railway infrastructure remains highly efficient, globally interoperable, and decisively resilient against the cyber threats of the future.

Works cited

1. [PDF] Railway Cyber-Security in the Era of Interconnected Systems,
<https://www.semanticscholar.org/paper/689ed86584eec24fa477486fa14926e5269afb82>
2. Why rail cybersecurity requires a different security model - Alstom,
<https://www.alstom.com/stories/why-rail-cybersecurity-requires-different-security-model>
3. Cybersecurity and Risk Management in Implementing Future,
<https://aaltodoc.aalto.fi/bitstreams/3875861a-e6b0-4857-a9d9-9a38c7cb5423/download>
4. Rail Cybersecurity in 2026: What the UK Market Data Tells ... - CYJAX,
<https://www.cyjax.com/resources/blog/rail-cybersecurity-in-2026-what-the-uk-market-data-tells-us-about-a-sector-under-pressure>
5. ENISA PUBLISHES 2025 EU CYBERSECURITY THREAT,
<https://www.clecat.org/news/newsletters/enisa-publishes-2025-eu-cybersecurity-threat-lands>
6. ENISA Threat Landscape 2025 - European Union,
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
7. ENISA 2025 Threat Landscape report highlights EU faces escalating,
<https://industrialcyber.co/reports/enisa-2025-threat-landscape-report-highlights-eu-faces-escalating-hackivist-attacks-and-state-aligned-cyber-threats/>
8. Rail cybersecurity must be bolstered against ransomware attacks, IT,
<https://industrialcyber.co/features/rail-cybersecurity-must-be-bolstered-against-ransomware-attacks-it-ot-integration-geopolitical-tensions/>
9. Cybersecurity Challenges in Modern Railway Signaling - IJFMR,
<https://www.ijfmr.com/papers/2025/5/56254.pdf>
10. Cyber Threat Post & Advisory - Varutra Consulting,
<https://www.varutra.com/ctp/index.php>
11. 2023 Cyber Security Report | PDF - Scribd,
<https://www.scribd.com/document/625693314/2023-cyber-security-report>
12. Microsoft Digital Defense Report,
https://www.nsr-org.no/uploads/documents/Publikasjoner/MDDR_FINAL_2023_10_04.pdf
13. CAE - Rail Code of Practice | Build it Secure | NPSA,
<https://www.npsa.gov.uk/security-best-practices/build-it-secure/cae-rail-code-practice>
14. From Conventional to Modernised ERTMS Level 2: Steps Towards,
<https://www.mdpi.com/2071-1050/18/3/1535>
15. A Systematic Development of a Secure Architecture for The,
<https://etheses.bham.ac.uk/id/eprint/8991/19/Thomas2019PhD.pdf>
16. An Attack Against Message Authentication in the ERTMS Train to,
https://www.researchgate.net/publication/315856296_An_Attack_Against_Messag

- [e_Authentication_in_the_ERTMS_Train_to_Trackside_Communication_Protocols](#)
17. Systematic Cybersecurity Risk Analysis of European Rail ... - arXiv,
<https://arxiv.org/pdf/2606.11839>
 18. A comprehensive study on cyberattack resilience for high-speed,
https://www.researchgate.net/publication/407067714_A_comprehensive_study_on_cyberattack_resilience_for_high-speed_train_security_protection
 19. Systematic Cybersecurity Risk Analysis of European Rail Traffic,
<https://arxiv.org/html/2606.11839v2>
 20. FRMCS Cybersecurity at Railroad-Road Crossings: Threat Model,
<https://www.mdpi.com/2071-1050/18/18/9665>
 21. TSN in the railway sector: why, what and how? | Industrial Ethernet,
<https://industrialethernet.net/tsn-in-the-railway-sector-why-what-and-how/>
 22. Westermo solutions for onboard rail networks | PDF - Slideshare,
<https://www.slideshare.net/slideshow/westermo-solutions-for-onboard-rail-networks/238339742>
 23. SecDT: A Profile-Based Security Layer for TRDP Communications,
<https://arxiv.org/html/2609.03133v1>
 24. (PDF) SecDT: A Profile-Based Security Layer for TRDP,
https://www.researchgate.net/publication/413964906_SecDT_A_Profile-Based_Security_Layer_for_TRDP_Communications
 25. EULYNX System Architecture Overview | PDF - Scribd,
<https://www.scribd.com/document/898588033/20240618-EULYNX-System-Definition-Eu-Doc-7-v4-2-2-A>
 26. EULYNX Deep Dive Security Course - Digital Transit,
<https://www.digitaltransit.co.uk/blog/eulynx-deep-dive-security-course/>
 27. Mipro OCS – Object Controller System,
<https://mipro.fi/en/rail-traffic/railway-solutions-and-references/mipro-ocs-object-controller-system/>
 28. EULYNX-Based Object Controller and CTC System in the Digirail,
<https://railway-news.com/mipro-eulynx-based-object-controller-and-ctc-system-in-the-digirail-project/>
 29. in Deutschland - Trackomedia,
https://www.trackomedia.com/media/e8/09/a0/1742412126/ETCS_in_DE_2024_Lesep.pdf
 30. Frauscher Point Control System Overview | PDF | Sensor | Computer,
<https://ro.scribd.com/document/816637908/2024-09-Point-Control-System-En>
 31. TRAKS: A Universal Key Management Scheme for ERTMS,
<https://cypherpunk.nl/papers/acsac17.pdf>
 32. Lantech OS5 Management Functions - Digitalical,
<https://digitalical.com/wp-content/uploads/2026/03/D-OS5-1.pdf>
 33. BS en 50129 - 2018 - Safety Related Systems For Electronic ... - Scribd,
<https://www.scribd.com/document/850612791/BS-en-50129-2018-Safety-Related-Systems-for-Electronic-Signalling>

34. Verified Directory of EU Rail Regulations & Standards - Railex,
<https://railex.eu/standards>
35. CAE - Rail Code of Practice Appendices | Build it Secure | NPSA,
<https://www.npsa.gov.uk/security-best-practices/build-it-secure/cae-rail-code-practice-appendices>
36. How to protect Railway organizations that have legacy systems from cyber attacks.docx
37. eug eulynx ocora rca - Security Guideline - EEIG ERTMS Users Group,
https://ertms.be/wp-content/uploads/2023/04/EULYNX_EUG_RCA_OCORA_Security_Guideline_v2.01.pdf
38. Understanding IEC 62443-3-2 Zones, Conduits, and Risk ... - Novesh,
<https://novesh.com/blog/novesh-blog-7/understanding-iec-62443-3-2-zones-conduits-and-risk-assessments-27>
39. Security Aspects of Zones and Conduits in IEC 62443 - MDPI,
<https://www.mdpi.com/2624-800X/6/2/52>
40. How to conduct an IEC 62443-based assessment for metro rail,
<https://shieldworkz.com/blogs/how-to-conduct-an-iec-62443-based-assessment-for-metro-rail-infrastructure>
41. A Practical Guide to Risk Assessment in ICS/OT using IEC 62443-3.2,
<https://medium.com/@sathish95/a-practical-guide-to-risk-assessment-in-ics-ot-using-iec-62443-3-2-c3fb43471e67>
42. IEC 63452: Railway Cybersecurity Standard | PDF - Scribd,
<https://www.scribd.com/document/838848675/03SRIS-1-IEC-PT-63452>
43. CLC/TS 50701 Railway Cybersecurity Overview | PDF - Scribd,
<https://www.scribd.com/document/713110977/CLC-TS50701-2021-e>
44. (PDF) Railway Infrastructure Cybersecurity: An Overview,
https://www.researchgate.net/publication/381651585_Railway_Infrastructure_Cybersecurity_An_Overview
45. IEC 63452 Railway Cybersecurity Standard | PDF - Scribd,
<https://www.scribd.com/document/838848677/session-3-1-iec-pt-63452-update-serge-benolie>
46. NIS2 Directive's Impact on Finland's Rail Cybersecurity | PDF - Scribd,
<https://www.scribd.com/document/916512870/The-Impact-of-the-NIS2-Directive-on-the-Cybersecurity>
47. European Rail Supply Industry - UNIFE,
https://www.unife.org/wp-content/uploads/2024/01/UNIFE_Annual_Report_2023.pdf
48. Rail Cyber Security Standards & Compliance Mapping - RazorSecure,
<https://www.razorsecure.com/standards-compliance>
49. Control Command and Signalling TSI,
https://www.era.europa.eu/domains/technical-specifications-interoperability/control-command-and-signalling-tsi_en
50. Saudi Arabia Cybersecurity & NCA Framework | Vision 2030,

- <https://vision2030.ai/sectors/technology/cybersecurity/>
51. Saudi Railway Company - LeadIQ,
<https://leadiq.com/c/saudi-railway-company/5a1d8b0b240000240065e18e>
 52. NCA Compliance Consulting Services In Saudi Arabia | Wattlecorp,
<https://www.wattlecorp.com/sa/services/nca-compliance/>
 53. NCA ECC MFA Compliance: Requirements, Implementation & Best,
<https://www.logintc.com/mfa-compliance/nca/>
 54. Understanding Saudi Arabia's Critical Systems Cybersecurity,
<https://genesisplatform.co/blogs/understanding-saudi-arabia-s-critical-systems-cybersecurity-controls>
 55. Saudi NCA OT Cybersecurity Guide | PDF | Computer Security - Scribd,
<https://www.scribd.com/document/849685684/Saudi-Nca-Otcc-Mapping-Guide-Txone-Wp-V>
 56. Essential Cybersecurity Controls (ECC) - CYBEROPS,
<https://cyberops.sa/nca-ecc/>
 57. 10 sectors in Jordan classified as critical infrastructure: NCSC,
<https://en.ammonnews.net/article/80294>
 58. ANNEX C1: Twinning Fiche EU funded project TWINNING TOOL,
<https://www.esteri.it/wp-content/uploads/2023/06/Annex-C1-Cybersecurity-Twinning-Fiche.pdf>
 59. Towards Effective Cybersecurity Governance: Jordan Compliance,
<https://www.mdpi.com/2624-800X/6/2/60>
 60. Israel's Relations with Arab Countries: The Unfulfilled Potential,
<https://mitvim.org.il/wp-content/uploads/2021/01/Israels-Relations-with-Arab-Countries-The-Unfulfilled-Potential-January-2021-Eng.pdf>
 61. Jordan National Railway Project - Amman,
https://www.mot.gov.jo/EBV4.0/Root_Storage/AR/Studies_Reports_AR_/General_Brochure_2011_08_04_Final_v2.PDF
 62. 2015 Achievements of ASEZ,
https://aseza.jo/ebv4.0/root_storage/ar/eb_list_page/achievements_report_2015.pdf
 63. Data Collection Survey on Trade and Logistics in Jordan, Palestine,
<https://openjicareport.jica.go.jp/pdf/12320149.pdf>
 64. Alstom invests in railway cybersecurity specialist Cylus and signs,
<https://www.alstom.com/press-releases-news/2020/12/alstom-invests-railway-cybersecurity-specialist-cylus-and-signs>
 65. Cyber Security For Rail System Suppliers | RazorSecure,
<https://www.razorsecure.com/system-suppliers>
 66. Railway Cybersecurity Market Report 2026-2031 by Solution,
<https://www.marketsandmarkets.com/Market-Reports/railway-cybersecurity-market-128598673.html>
 67. Cybersecurity Archives - Railway Technology,
<https://www.railway-technology.com/sector/theme/technology/cybersecurity/>

68. Alstom investing \$7 million in Israeli rail cyber protection startup Cylus,
<https://www.calcalistech.com/ctech/articles/0.7340.L-3880348.00.html>
69. Alstom and the Rochester Institute of Technology's ESL Global,
<https://www.alstom.com/press-releases-news/2023/1/alstom-and-rochester-institute-technologys-esl-global-cybersecurity-institute-sign-memorandum-understanding>