ARMIS®

SOLUTION BRIEF

Securing Rail Networks and Adhering to Rail Security Directives with Armis Centrix™

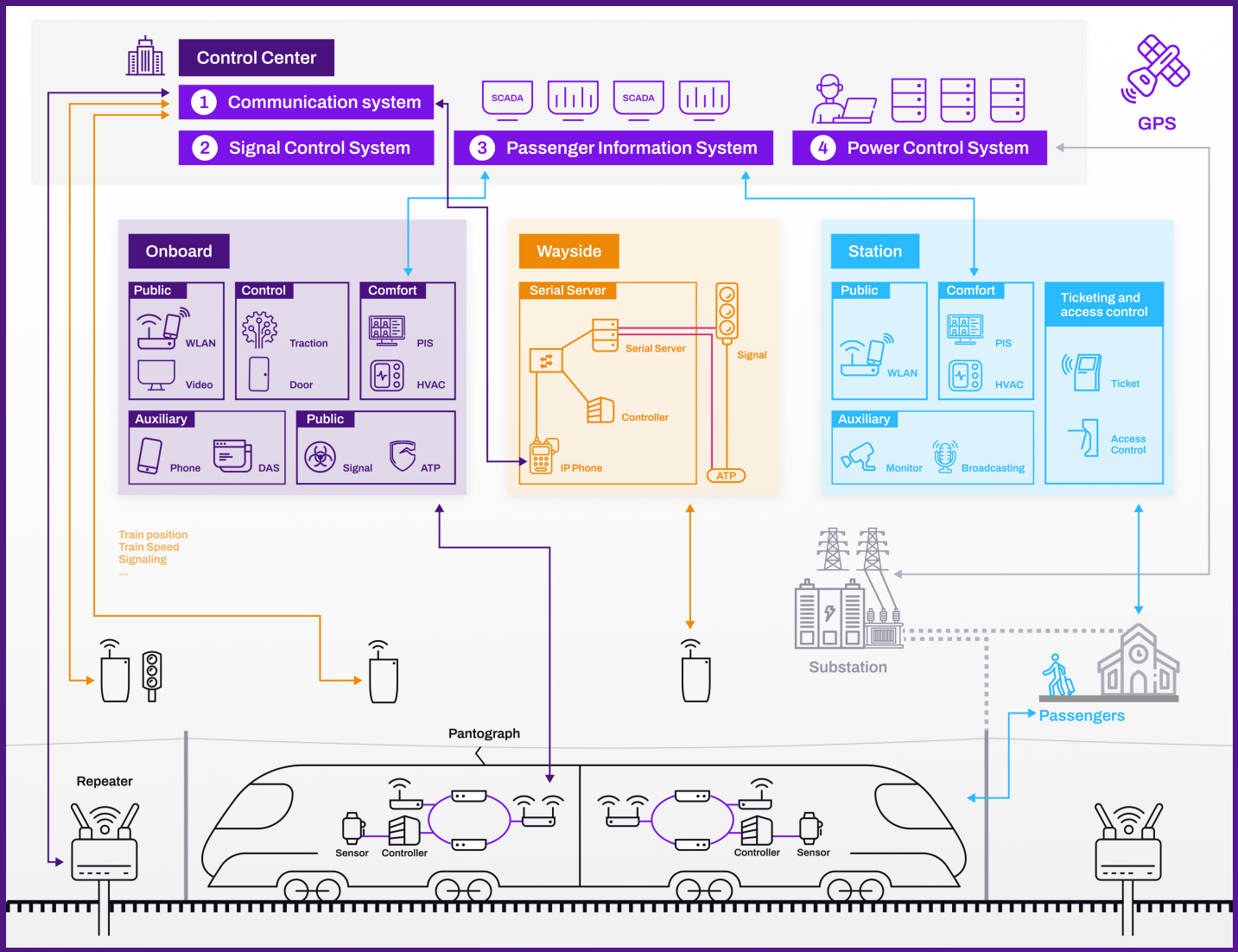
Executive Summary

From operational signalling and rolling stock controls to station systems and passenger-facing services like ticket gates, in regions such as the US and Europe networks have been dependent on digital systems for many years. Recent incidents (notably the Critical cyber flaw linked to EoT module.) demonstrate how relatively low-effort attacks or insider misuse can disrupt services and undermine public confidence. Effective cyber security for rail must therefore combine safety-informed risk management, sector-specific controls, and alignment with national frameworks such as the TSA Rail Cybersecurity Directive (SD 1580/82-2022-01), NIS2 or the NCSC Cyber Assessment Framework (CAF).

Challenges Faced in the Rail Industry

Rail systems are critical national infrastructure where cyber failures can cause not only data loss but also safety incidents and large-scale disruption. Key characteristics that make rail distinct:

- **Safety-critical coupling:** Operational technology (OT) systems (signalling, interlocking, train-borne control) link directly to safety outcomes.
- **Heterogeneous legacy estate:** Many assets are long-lived and were not designed with cybersecurity in mind. Upgrading or replacing them is complex and costly.
- **Complex supply chain:** Systems are developed, deployed and maintained by multiple OEMs, integrators and third-party service providers, increasing dependency and risk.
- **Public-facing services:** Passenger Wi-Fi, ticketing portals and real-time information services create reputational and privacy exposure.
- **Safety vs. Security Trade-offs:** Rail culture prioritizes fail-safe operations, but incident containment often requires fail-secure actions.
- **Highly complex environments** with constant moving parts.



Threat Landscape in the Rail Industry

Rail operators face a spectrum of threats. Typically, the speed of exploitation, safety concerns and the high likelihood of reputational damage make rapid detection and remediation paramount.

- Nation-state and advanced persistent threats (APTs): Motivated actors seeking disruption or espionage against critical infrastructure.
- Cybercriminals and ransomware groups: Seeking financial gain through disruptive malware or extortion.
- Insider threats and supply-chain compromise: Malicious or negligent insiders and compromised third parties can cause targeted or opportunistic incidents.
- Opportunistic vandalism and misconfiguration: Lower-skill attackers or administrative errors can still cause wide impact, especially against poorly segmented or externally accessible systems.

Regulatory Frameworks Impacting the Rail Industry

Rail operators face a spectrum of threats. Typically, the speed of exploitation, safety concerns and the high likelihood of reputational damage make rapid detection and remediation paramount.

NIS2: Requires railway operators and infrastructure managers to implement robust cybersecurity risk management and incident reporting measures, ensuring the resilience and protection of critical network and information systems used in rail transport.

EN 50126: Defines the railway **RAMS lifecycle** for system safety and reliability.
EN 50128: Sets **software safety** requirements for railway control systems.
EN 50129: Specifies the **safety case** process for signaling systems.
EN 50159: Ensures **secure communication** in railway signaling networks.

TSA Directive SD 1580/82-2022-01: It is performance-based, meaning it sets outcomes or goals that rail operators must meet, rather than prescribing every technical detail. It applies to freight and passenger railroad owner/operators.

Department for Transport (DfT) rail cyber guidance: High-level guidance for protecting safety- and reliability-critical rail systems. It sets principles for risk management and system lifecycle considerations.

NCSC Cyber Assessment Framework (CAF): A comprehensive, outcome-focused framework for assessing cyber maturity across governance, protection, detection and response activities; increasingly referenced by regulators and operators.

RSSB technical notes and standards (e.g., TN2312): Rail-specific technical guidance addressing rolling stock cyber essentials and engineering controls. These bridge OT/IT safety concerns and practical engineering measures.

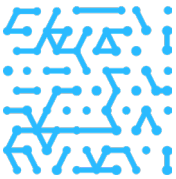
Regulatory engagement (ORR and others): The Office of Rail & Road continues to work with industry to ensure appropriate preparedness and reporting for cyber threats.

Operators should treat these documents as complementary: national frameworks provide assessment and governance models, while sector guidance translates those into rail-specific engineering and operational expectations.

Key Vulnerabilities Observed in Rail

When we look at recent public incidents and reports on how rail has been breached, common weak points include:

- **Weak administrative controls on shared/third-party services:** Misuse of an administrative account on a supplier platform can impact supplier access and weak privileged-account controls.
- **Insufficient network segmentation between passenger/IT and OT networks:** Poor separation can allow attackers who initially target passenger services to pivot into operational systems.
- **Legacy protocols & unpatched systems:** Long-lived signalling and rolling stock components often rely on outdated protocols and have constrained patching windows.
- **Supply-chain opacity:** Limited visibility of supplier cybersecurity practices increases risk of third-party compromise.
- **Limited detection & response capability for OT:** Many operators lack rapid detection tailored to OT behaviours, slowing containment and recovery.



Practical Playbook Recommendations

Strategic (board/executive).

- **Treat cyber as safety & operational risk:** Include cyber in safety cases and operational risk registers; require cyber risk reporting to boards and regulators. (Aligns with DfT guidance.)
- **Adopt CAF as the assessment backbone:** Use NCSC CAF to assess and prioritize investments across governance, protection, detection and response.

Tactical (operator/SOC/engineering)

- **Zero Trust segmentation:** Implement strict network segmentation and least-privilege access between passenger IT, corporate IT and OT networks. Include micro-segmentation where appropriate.
- **Privileged access management & supplier controls:** Harden administrative access (zero trust), mandate supplier security baselines and perform regular access reviews.
- **OT-aware detection & incident playbooks:** Deploy detection tuned to OT protocols and behaviours, and test OT incident response regularly (tabletops, live exercises).
- **Secure procurement & lifecycle engineering:** Require cyber security clauses in contracts, evidence of secure development practices, and adherence to rail-specific standards such as RSSB technical notes when acquiring rolling stock or control equipment.

Operational (daily operations)

- **Patch & configuration management windows:** Define safe, auditable processes to apply security updates to OT where feasible; where not feasible, mitigate with compensating controls (segmentation, monitoring).
- **Data minimization & privacy hygiene:** Limit personal data exposure on passenger systems and apply standard DLP controls to reduce privacy risk in case of compromise.
- **Cross-industry information sharing:** Participate in sector CSIRTs, the rail industry sharing forums, and NCSC-led initiatives to share indicators and response playbooks quickly.

Real World Example- Cybersecurity flaw in End-of-Train (EoT) modules

Earlier this year, U.S. rail systems faced growing scrutiny after researchers revealed that a critical cybersecurity flaw in End-of-Train (EoT) modules had been ignored for over a decade. The vulnerability, first identified in 2012, allows attackers using low-cost software-defined radios to intercept or spoof train brake commands, posing risks of derailments or system-wide shutdowns.

Despite repeated warnings, the Association of American Railroads (AAR) delayed action, claiming the devices were nearing end of life. After public disclosure and pressure from researchers, the Cybersecurity and Infrastructure Security Agency (CISA) issued a formal advisory in July 2025 confirming the flaw, now tracked as CVE-2025-1727, and rating it as high severity. The AAR has since announced plans to replace vulnerable equipment and protocols by 2027, but the slow response has raised concerns about cyber risk management and accountability within critical infrastructure sectors.

How Armis Centrix™ Delivers Security for Rail

Deep Asset Discovery & Visibility

Rail environments run on a mix of legacy signalling, SCADA, OT IoT, and IT systems, many of which are undocumented or unmanaged. Armis automatically discovers every connected asset across trackside, rolling stock, depots, and stations without disrupting operations. With OT protocol integrations and Smart Active Querying (SAQ), even sensitive signalling and interlocking systems are safely interrogated, giving operators a trusted single source of truth for security and operational awareness.

Preemptive Threat Detection & Early Warning

Rail environments run on a mix of legacy signalling, SCADA, OT IoT, and IT systems, many of which are undocumented or unmanaged. Armis automatically discovers every connected asset across trackside, rolling stock, depots, and stations without disrupting operations. With OT protocol integrations and Smart Active Querying (SAQ), even sensitive signalling and interlocking systems are safely interrogated, giving operators a trusted single source of truth for security and operational awareness.

Vulnerability Prioritization & Fast Remediation

Not every vulnerability poses the same risk to a rail network. Armis maps vulnerabilities to device role and criticality, from safety-critical signalling equipment to passenger Wi-Fi routers, helping prioritize the exposures that truly matter. Integrated patch workflows, compensating controls, and automated rollback ensure faster, more effective remediation, while executive risk scoring aligns cyber priorities with safety and business outcomes.

Segmentation & Secure Access Control

Rail networks depend on numerous contractors and suppliers for rolling stock, station systems, and trackside assets. Armis enforces network segmentation between IT and OT, while also applying dynamic micro-segmentation around signalling and train control systems to protect mission-critical assets. Secure vendor access is enabled with just-in-time policies, while compensating controls that leverage NAC, SIEM, firewalls etc. ensure every connection, whether by staff, suppliers, or systems, is tightly monitored and controlled.

Safeguarding Service & Process Integrity

Unplanned downtime in rail means delayed timetables, safety risks, and passenger disruption. Armis safeguards process integrity by identifying obsolete, end-of-life systems that pose hidden risks. It detects tampering or abnormal behavior in signalling and SCADA early, ensuring disruptions are prevented before they cascade. Change control verification ensures only authorized updates occur, protecting both safety-critical operations and passenger confidence.

Compliance & Regulatory Alignment

Rail operators globally must meet strict regulatory expectations from TSA, NCSC Cyber Assessment Framework (CAF), Department for Transport (DfT), and NIS2. Armis maps vulnerabilities and risks directly to these requirements, continuously monitoring compliance status. Automated evidence collection and live dashboards simplify audit preparation, providing executives and regulators with ongoing assurance that cyber risk is managed to the same standard as safety.

Deeper Dive: TSA Directive

How Armis Aligns with TSA's Rail Cybersecurity Directive

TSA Directive Requirement	Description/Objective	How Armis Supports Compliance
Cybersecurity Implementation Plan (CIP)	Develop and maintain a TSA-approved plan for achieving cybersecurity objectives.	Armis provides a unified asset inventory and continuous risk assessment data that can be directly incorporated into a CIP. Dashboards and reports from Armis can demonstrate compliance readiness and ongoing adherence to TSA requirements.
Network Segmentation & Access Controls	Segment IT and OT networks to prevent compromise spread and restrict access to critical cyber systems.	Armis maps all connected assets and their communications in real time, identifying unauthorized connections or segmentation violations. It enforces network segmentation while also initiating dynamic device micro-segmentation. It also highlights high risk lateral communications to support segmentation design and validation.
Continuous Monitoring & Threat Detection	Continuously monitor networks and systems for suspicious activity or anomalies.	Armis delivers continuous monitoring across IT, OT, and IoT environments, detecting anomalous behavior, unpatched devices, or unauthorized access — fulfilling the directive's monitoring and detection mandate.
Patch Management & Vulnerability Mitigation	Identify and remediate vulnerabilities and apply patches to reduce cyber risk.	Armis automatically identifies devices with outdated firmware or missing patches and prioritizes them by risk context (criticality, exposure, exploitability). It can feed data into patch management and/or ticketing systems for remediation tracking.

TSA Directive Requirement	Description/Objective	How Armis Supports Compliance
Cybersecurity Assessment Program (CAP)	Regular testing and auditing of cybersecurity controls, at least every 3 years.	Armis enables automated control validation by continuously assessing asset posture and configuration. Reports from Armis can serve as evidence in periodic TSA assessments or internal audits.
Incident Response Exercises	Conduct annual cybersecurity incident response drills and document findings.	Armis integrates with SIEM/SOAR tools (e.g., Splunk, Sentinel, Cortex XSOAR) to simulate and respond to incidents, providing detailed forensic data to support tabletop exercises and post-incident analysis.
Annual Reporting / Updates to TSA	Submit annual updates on cybersecurity status and assessment results.	Armis provides exportable compliance and asset posture reports suitable for submission to TSA or internal compliance documentation. These reports demonstrate continuous visibility and control improvements.
Protection of Positive Train Control (PTC) Components	Apply physical or cybersecurity controls to PTC systems to prevent compromise.	Armis detects and monitors network-connected PTC assets, ensuring only approved devices communicate. It can identify new or rogue devices that could threaten safety-critical systems.
Incident Detection & Notification (implied in all TSA directives)	Rapidly detect and notify TSA of cybersecurity incidents.	Armis accelerates incident detection through behavioral analytics and risk-based alerting. It integrates with ticketing and notification systems for automated rapid escalation and reporting.

Conclusion

Securing rail networks requires a blend of best practice (TSA, NCSC CAF), rail-specific engineering controls (RSSB/DfT guidance), and pragmatic operational steps focused on segmentation, privileged access, supplier assurance and OT detection. Recent incidents show that threats range from insider misuse to opportunistic vandalism, and that relatively simple controls (tight access management, clearer supplier contracts and better segmentation) can significantly reduce risk. By embedding solutions like Armis Centrix™, the sector can move beyond compliance to a proactive, intelligence-led security model. This ensures protection of passengers, continuity of services, and preservation of public trust.