IndraMind

A 360° Cybersecurity Approach to Protect Rail Systems

26 November 2025

IndraMind

Who am I?

www.linkedin.com/in/tarikbissan

The Digital Transformation of Rail

Modern rail systems are more connected, data-driven and software-defined than ever.

Digital Signalling

ETCS, CBTC, and modern interlockings shift control systems to fully digital platforms.

Smart Rolling Stock

Trains become connected nodes: onboard networks, diagnostics, telemetry, remote maintenance, and enhanced passenger services such as Wi-Fi connectivity, infotainment, real-time travel information, and smart ticketing.

Next-Generation Telecom

Railways migrate from legacy GSM-R to IP-based communication systems, including LTE-R in some regions, and towards future FRMCS/5G.

Integrated OCC

Signaling, SCADA, video, energy, and passenger systems converge into unified digital control rooms.

Connected Wayside

Trackside assets, points, signals, and sensors are now networked and remotely monitored.

Overall impact

- ✓ **Enhanced passenger experience** through digital services, and real-time information.
- ✓ **Greater operational and infrastructure efficiency** thanks to data-driven decision making.
- ✓ **Expanded cyber attack surface** requiring a rail-specific cybersecurity approach.

What Makes Rail Unique

Key characteristics that differentiate rail from other critical infrastructures.

These characteristics make the railway sector unique and fundamentally different from other OT environments.

Safety-Critical Environment

Operations prioritize safety above all. Any change must integrate with RAMS and follow strict safety assurance processes.

Long Procurement & Delivery Cycles

Rail procurement, certification and commissioning processes are long, highly regulated and involve multiple stakeholders—extending from tender to operation over several years.

Long Asset Lifecycles

Signaling, interlockings, telecom, and rolling stock remain in service for 20–40 years, creating strong technology heterogeneity.

Highly Distributed Infrastructure

Rail systems span long distances: tracks, stations, tunnels, depots, OCCs wide physical exposure and complex topology.

Safety-Driven Change Control

Updates and patching require careful engineering and coordination, and any change affecting RAMS or safety functions may trigger re-assessment or re-certification.

Interoperability Challenges

Multiple OEMs, technologies, interfaces, and system variants make integration challenging.

Rail Cybersecurity Challenges

- **Safety ≠ Security**: safety mechanisms (fail-safe, redundancy, overrides) protect operations but can be abused by attackers and do not guarantee cybersecurity.
- **Legacy, long-lifecycle systems**: interlockings and other safety-critical components run on old platforms, and extremely long-life cycles, from procurement to operation, make it hard to keep security up to date.
- **Exposed protocols and wireless links**: proprietary signaling protocols and their communication channels, especially legacy radio technologies such as GSM-R, and unprotected Wi-Fi links used in CBTC/ERTMS, were not designed with modern cyber threats in mind.
- **Fail-safe and irregular operations as DoS enablers**: principles like “stop in case of doubt” and emergency overrides can be deliberately triggered to cause repeated service disruption.
- **Broken air-gaps and misconfigurations**: unintended links and remote access often connect OT to IT, so operational networks are not as isolated as they appear.
- **Human factors and long-life cycle**: configuration mistakes, limited cyber awareness in operations and 30-year system lifetimes make maintaining security over time a continuous challenge.

Why Rail Needs a Specific Cybersecurity Approach?

- **Safety-critical operations**: rail systems are designed for passenger safety, not for cyber resilience. Any malicious command can trigger fail-safe stops or disrupt service.
- **Highly distributed, long-life infrastructure**: rail assets operate for 20–30+ years, combining legacy and modern systems. They are spread across large, hard-to-secure areas (e.g., trackside equipment, cable ducts), making protection and updates slow and complex.
- **Growing digital attack surface**: increasing connectivity (OT/IT integration, remote access, wireless links) creates new entry points that did not exist in legacy architectures.
- **Complex multi-vendor ecosystem**: different OEMs, protocols and integration models complicate consistent security controls across trains, signaling, stations, and depots.

Safety-critical nature

Rail cannot operate under “best effort”; failures impact on people.

Long asset lifecycles

Technology evolves faster than rolling stock and signaling.

Operational continuity

Service must run 24/7, limiting changes, patching and downtime.

Distributed architecture

Trains, interlockings, RBCs, stations, depots, wayside, high exposure.

Regulated environment

Cybersecurity measures must coexist with Safety (RAMS) and Certification.

The Evolving Threat Landscape

Key Observations:

- Ransomware remains the highest-impact threat for transport operators.
- Increasing attacks on suppliers, and maintenance ecosystems.
- Growing focus on OT reconnaissance, and network infiltration in rail systems.
- Credential theft is one of the most common entry vectors in rail incidents.
- State-sponsored groups continue to target European critical infrastructure. AI-powered tools amplify phishing, fraud, social engineering, and malware creation.

Nation-State Activity

State-sponsored campaigns targeting transport and critical infrastructure for disruption, intelligence or pre-positioning.

Ransomware on Critical Operators

Targeting operators, infrastructure managers and suppliers, driven by high impact and high likelihood of payment.

Credential Theft & Access Abuse

Stolen VPN credentials, remote-access abuse, and weak authentication enabling intrusion into corporate or operational networks.

Supply Chain Attacks

Compromise of signaling/rolling-stock vendors, maintenance providers or software updates to gain access to operational environments.

OT Network Intrusions

Focused attempts to map, infiltrate or disrupt signaling, interlocking, wayside and depot systems.

Insider & Contractor Risk

Third-party technicians, maintenance teams, and contractors with privileged access.

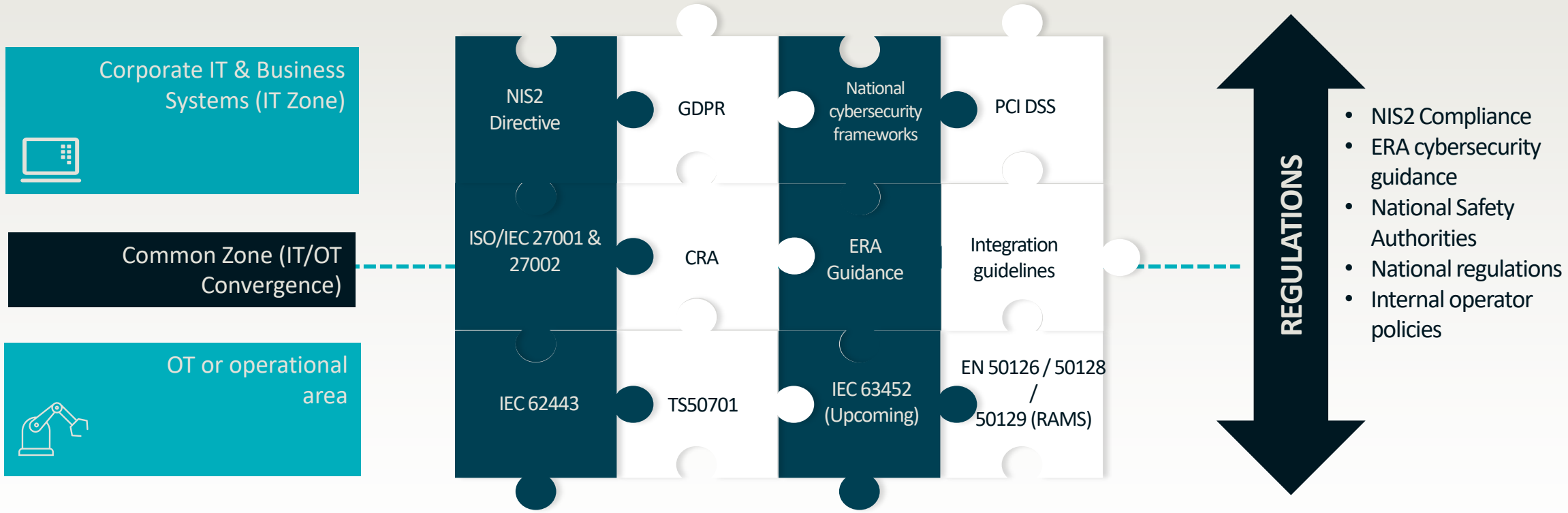
AI-Enhanced Cybercrime

Faster phishing, impersonation, malware development, and deepfakes increasing both speed and sophistication of attacks.

Threats observed in recent years are being amplified by AI, while adversaries are increasingly interested in operational disruption and supply chain compromise.

Rail Cybersecurity Standards & Regulation

Rail cybersecurity in Europe is guided by a mix of sector-specific standards and transversal regulations.
These frameworks define how signaling, rolling stock, telecoms, control centers, and other rail environments must be protected, ensuring cybersecurity aligns with safety requirements.



Our 360º Approach to Secure Railways

A holistic cybersecurity model that operates across all lines of defense and throughout every phase of the railway project and system lifecycle, fostering a culture of risk mitigation.

2LoD

Support and oversight of risk management

Governance & Risk Management

- Cybersecurity strategy aligned with safety
- Alignment with TS 50701, IEC 62443
- Third-party & supply-chain risk management
- Rail-specific security & change-control processes

Prevention

Reduce exposure across rail assets and operational systems.

- Rail asset inventory & topology mapping (wayside, onboard, OCC)
- Vulnerability assessment
- Secure-by-design for new projects & upgrades
- Cyber risk assessments
- Supplier and integrator security requirements

Protection

Harden critical systems and ensure secure operations.

- Deployment, operation and management of security technologies
- Network segmentation and perimeter security between IT, OT, OCCs, depots and stations
- Secure remote access
- Protection for operator and engineering workstations and mobile devices.
- Secure access networks
- Secure private and radio networks
- Secure architectures

Detection

Smart MDR (Managed Detection & Response)

Rail-aware monitoring to detect malicious activity early.

- Threat Intelligence: Identify cyber threats and campaigns targeting rail operators, suppliers and critical infrastructure, providing early-warning alerts.
- Security Monitoring & Incident Detection: 24x7 monitoring of IT and OT environments with use-case–based detection tuned to rail scenarios.
- Alert Management & 24x7 First Response: Continuous triage, notification, escalation and initial response actions, executed according to playbooks agreed with operations & safety teams.
- Threat Hunting: Proactive hunting to uncover stealthy attacks, misuse of engineering tools and anomalies.

Response

Coordinate rapid, safe and effective incident response.

- 24/7 cyber response for both IT and rail OT
- OT-forensic capability for signalling, telecom and onboard networks
- Crisis management integrating safety & operations
- Malware analysis and containment in safety-critical environments
- Railway cyber-range exercises for OCC, maintainers & operators

Recovery

Restore safe operations with minimal service disruption.

- Resilience and continuity plans for railway operations
- Backup & recovery for signalling data, OCC platforms and engineering tools
- Post-incident analysis integrated with safety case updates
- Lessons learned incorporated into operational procedures

IT

OT

Cloud

IA

Assessments

Adequacy

Audit

Supply and implementation of tools

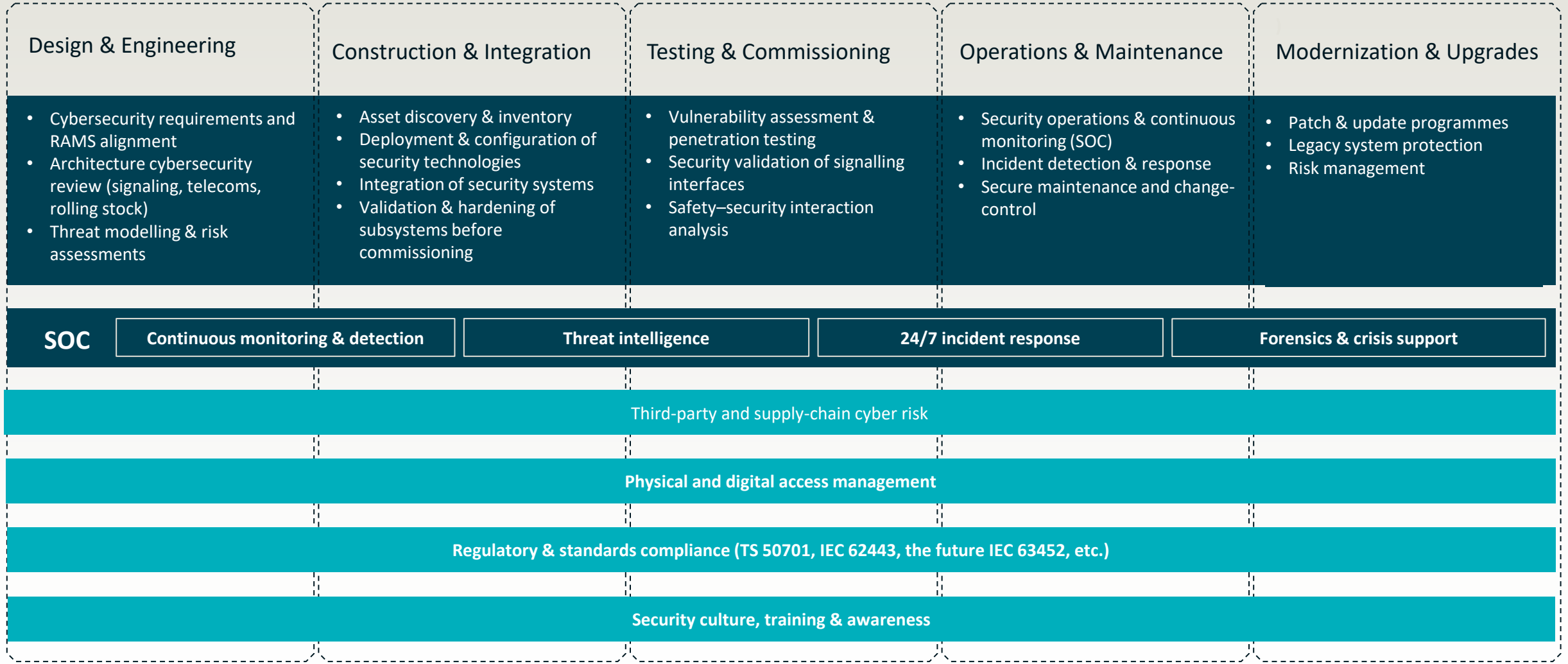
Managed services

1LoD

Operational and risk management

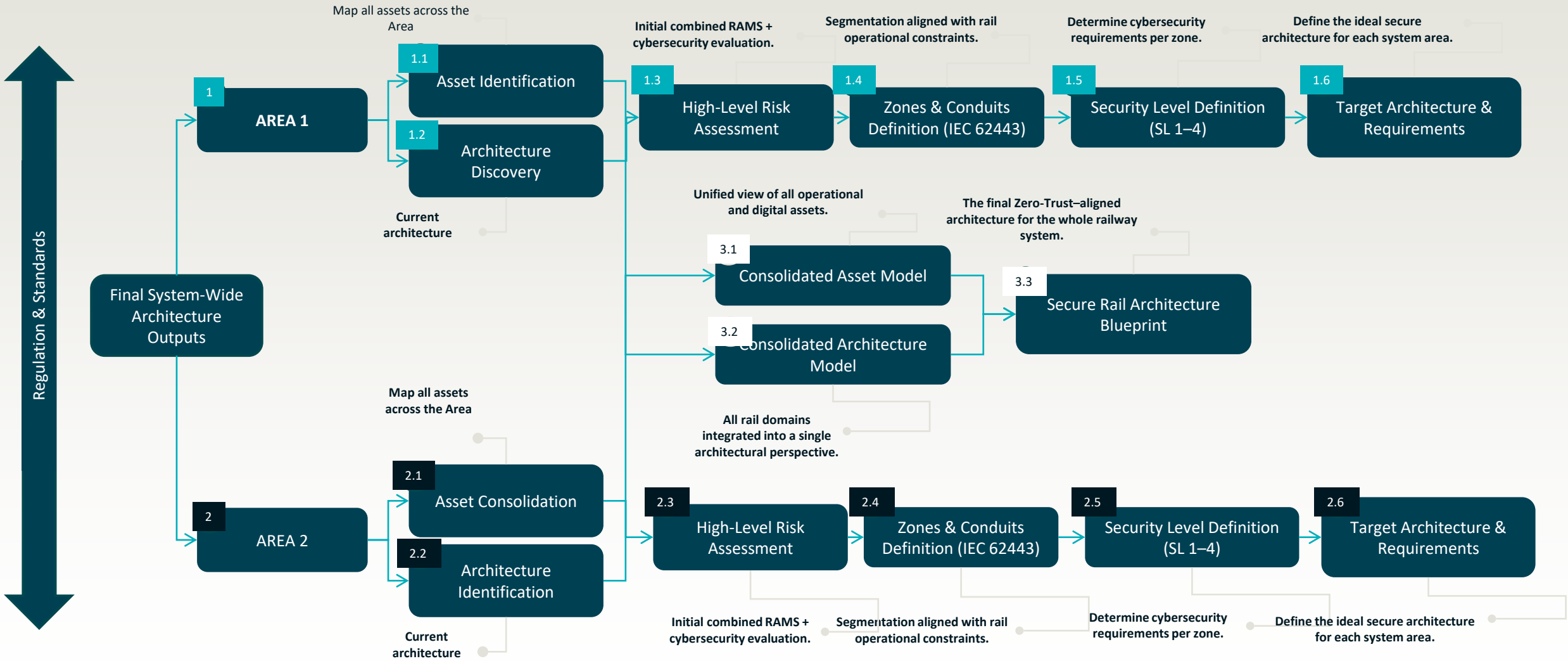
Our 360º Approach to Secure Railways

Rail Cybersecurity Across the Full System Lifecycle – Ensuring secure, resilient, and reliable operations from design to operation.



Our 360º Approach to Secure Railways

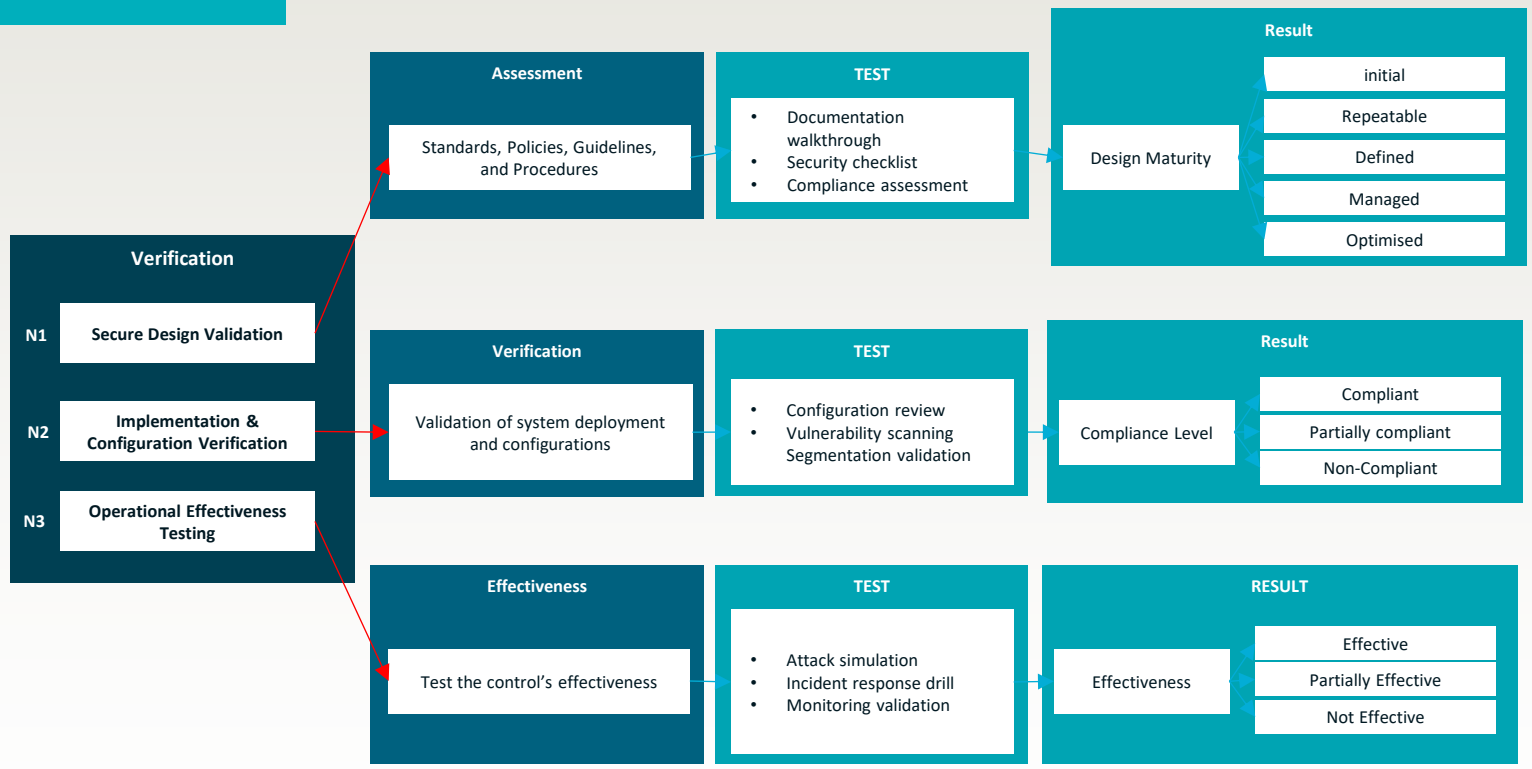
Building Secure Railway Architectures Across All Rail Domains



Our 360º Approach to Secure Railways

Ensuring cybersecurity validation throughout all phases of the railway project lifecycle reduces project risk, ensures compliance, and guarantees that systems enter service securely and resiliently.

VERIFICATION LEVELS



Ensure cybersecurity requirements are correctly embedded before construction and integration begin:

- Review of security requirements and technical specifications
- Validation of all rail areas architectures
- Zoning & conduits review (IEC 62443 / TS 50701)
- Documentation-based verification

Confirm that systems are built and configured securely during Construction & Integration:

- Architecture verification (network, interfaces, firewalls)
- Configuration review of deployed systems
- Hardening validation across suppliers
- Cyber checks during FAT & SAT

Validate that cybersecurity controls operate effectively under real conditions before entry into service:

- Penetration testing (safe-by-design scope)
- Red-team simulations and cyber-incident exercises
- SIEM/log/alert validation
- Backup, failover and recovery testing

Smart MDR
How We Operate

Our Managed Detection & Response service is designed to rapidly detect, contain and reduce the impact of cyber incidents, with measurable outcomes that strengthen the organizations' resilience over time.

We combine 24/7 monitoring, AI, threat intelligence, advanced analytics, and specialized response capabilities in a single managed service.

A collaborative, continuous-improvement cycle…

We work as an extension of the client's team, sharing visibility, decisions and priorities.
We constantly measure service performance to improve both efficiency and effectiveness.

… starting from relevant threat intelligence…

We obtain high-value insights on adversaries, campaigns and vulnerabilities that matter to your organization. We track threats on the internet and dark web and translate them into concrete detection rules and defensive actions.

Key capabilities

- Threat Intelligence (global & sector-specific)
- IOC and TTP enrichment for SIEM / EDR / OT monitoring
- Early-warning on emerging vulnerabilities and exploits

… we help reduce the attack surface…

We identify exposed assets and weak points, communicate new vulnerabilities, prioritize them and recommend how to fix them.

We support clients in designing and implementing robust security controls.

Key capabilities

- Attack surface assessment & continuous exposure management
- Vulnerability management & prioritization
- Security configuration reviews & hardening
- Use-case design for detection

… we detect attacks in real time…

Using automated and orchestrated detection scenarios, complemented with proactive threat hunting,
we identify malicious behaviour across IT, OT and cloud environments..

Key capabilities

- 24/7 security monitoring based on use cases
- Correlation & analytics
- Proactive threat hunting (manual and automated)
- Deception techniques where applicable

… and we respond effectively

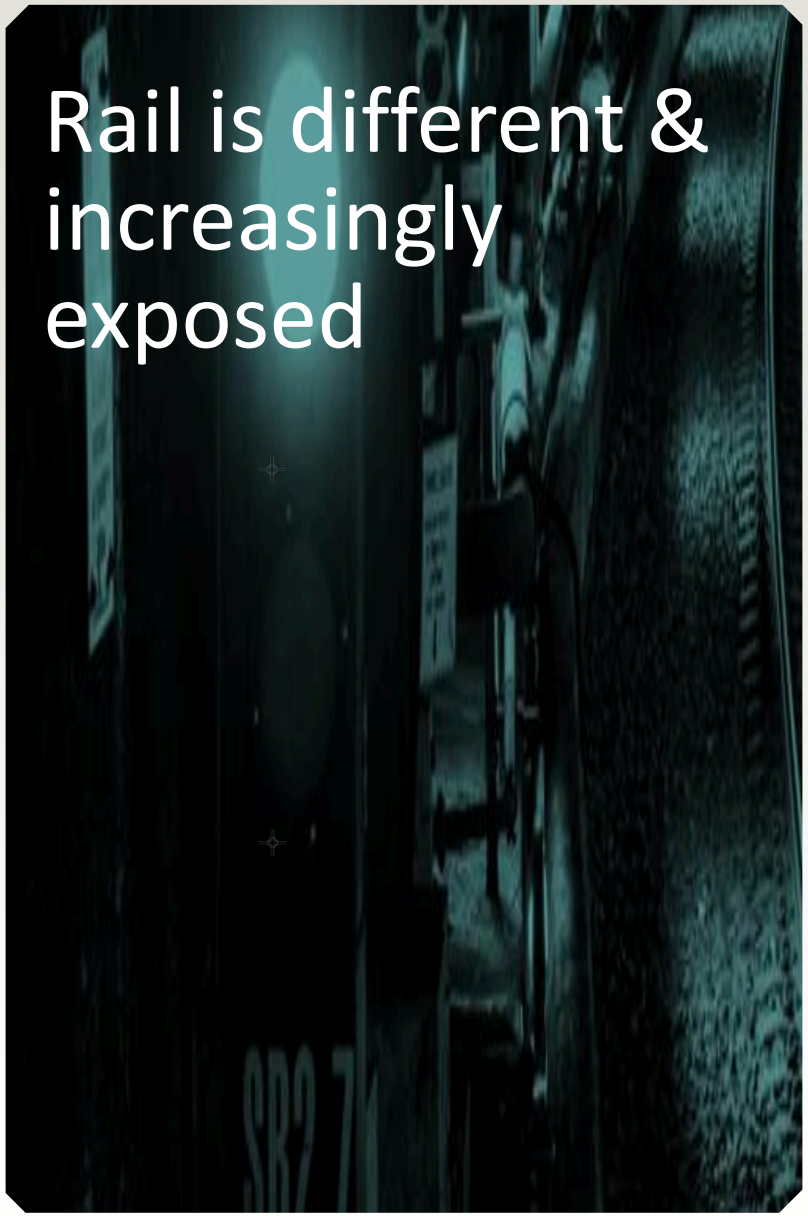
We give context to alerts, drastically reduce false positives and coordinate technical and business actions to contain and remediate incidents.

Key capabilities

- First response & incident triage 24/7
- Incident handling & crisis management support
- Digital forensics & incident response (DFIR)
- Incident readiness & playbook development
- Post-incident reviews and improvement actions

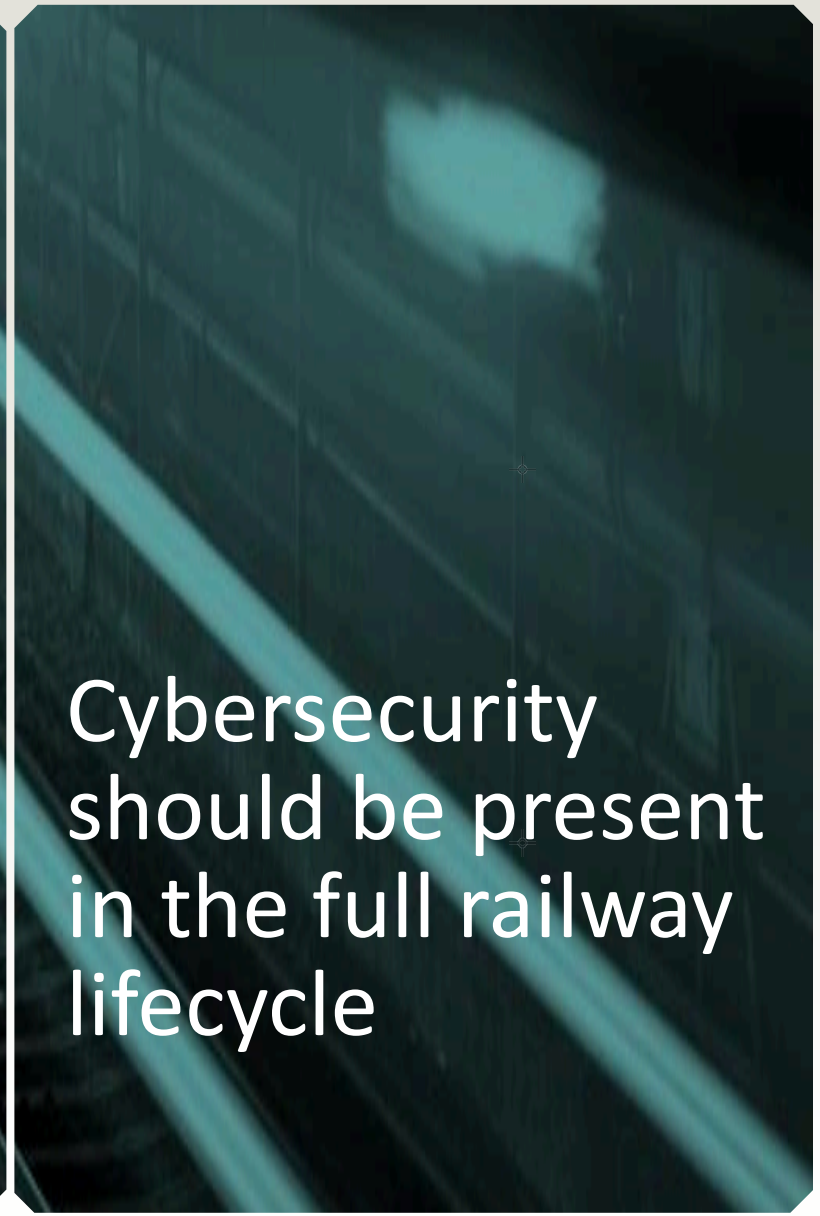
Protecting infrastructures and information across IT, OT and Cloud environments with a 24/7

Managed Detection & Response service



Rail is different & increasingly exposed

Cybersecurity must be rail-specific



Cybersecurity should be present in the full railway lifecycle


IndraMind