RAIL

Cyber Threats to Smart Railways

Today's smart railways use advanced digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, IP/optical networks, and 5G to make their operations run more efficiently and responsively than ever before. But this reliance on digitalization exposes smart railways to a number of cyber risks.

"Smart rail systems combine safety-critical, long-lifecycle assets (20–40 years), and rapidly evolving digital technologies, creating a risk profile that differs fundamentally from classical IT systems," said Eddy Thesee. He is digital and cyber platform vice president with Alstom, one of the world's largest manufacturers of railway vehicles, infrastructure, and transport systems. "These vulnerabilities remain poorly understood because cybersecurity effects are often latent: a digital weakness may exist for years before being weaponized, while safety certification tends to 'freeze' architectures, delaying security updates. This cultural and structural gap — between fast-moving cyber threats and conservative safety processes — is a systemic rail-specific challenge rather than a tooling issue."

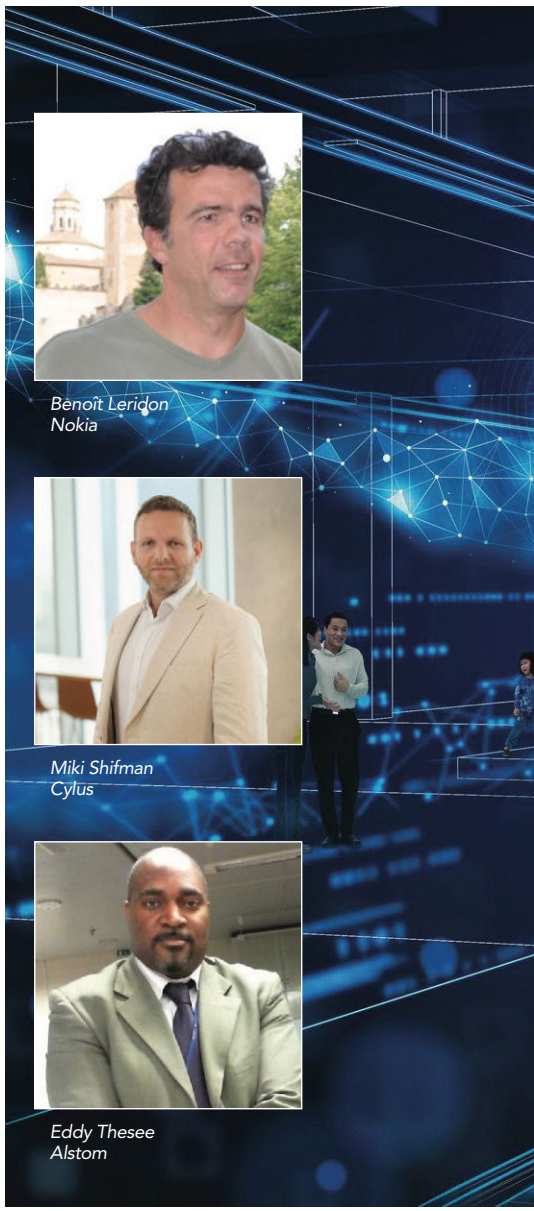
The Price of Uniqueness

As transportation systems go, smart railways are unique in combining many generations of technology into an integrated platform.

According to Miki Shifman, CTO and co-founder of Cylus — a company providing purpose-built cybersecurity for rail operational technology (OT) — the age of these systems is a major factor. "Rail is one of the few industries where the threat surface spans a century of technology," he said. "You have signaling logic running on equipment installed in the 1980s, sitting on the same network as IP-based train control systems and cloud-connected maintenance platforms. The attack surface keeps expanding as operators modernize piecemeal, but the legacy systems don't disappear. They get connected."

As a result, the cyber threats that confront smart railways have the potential to cripple their IT, OT, and operational safety systems simultaneously. "A network anomaly that would be a minor incident in a corporate environment can have direct physical consequences in a signaling network," Shifman told TSI. Additionally, "Most cybersecurity professionals don't know rail operations. Most rail engineers don't know cybersecurity. That gap is exactly where attackers operate."

That's not the only price of being different. "Railways are unique because their deployed telecom assets transport critical applications in locations where there is little or no protection, and their radio network can be reached

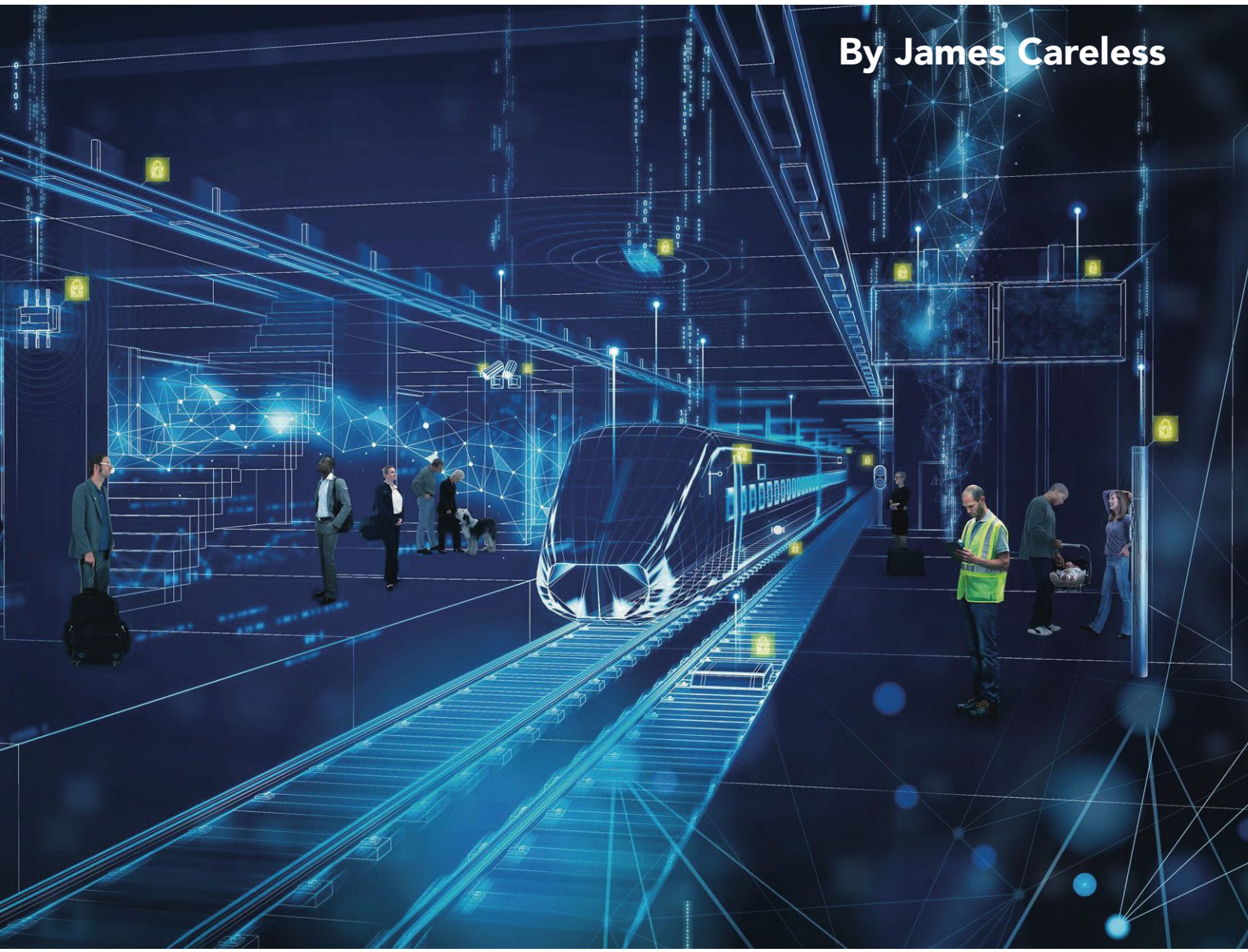


Benoît Leridon
Nokia

Miki Shifman
Cylus

Eddy Thesee
Alstom

Alstom says they have combined up-to-date IP communication technologies and the latest international interoperability standards in their Agate Net product, which provides wireless and onboard network communications. It concentrates cybersecurity monitoring and protection fully in line with IEC62443 and TS50701 standards to support safe and secure operations. Alstom image.



By James Careless

outside of protected sites," said Benoît Leridon, Nokia's transportation market leader for network infrastructure at Nokia, which equips smart railways with secure communication networks. "These vulnerabilities leave time for hackers to develop, test and realize attacks."

Several Attacks to Date

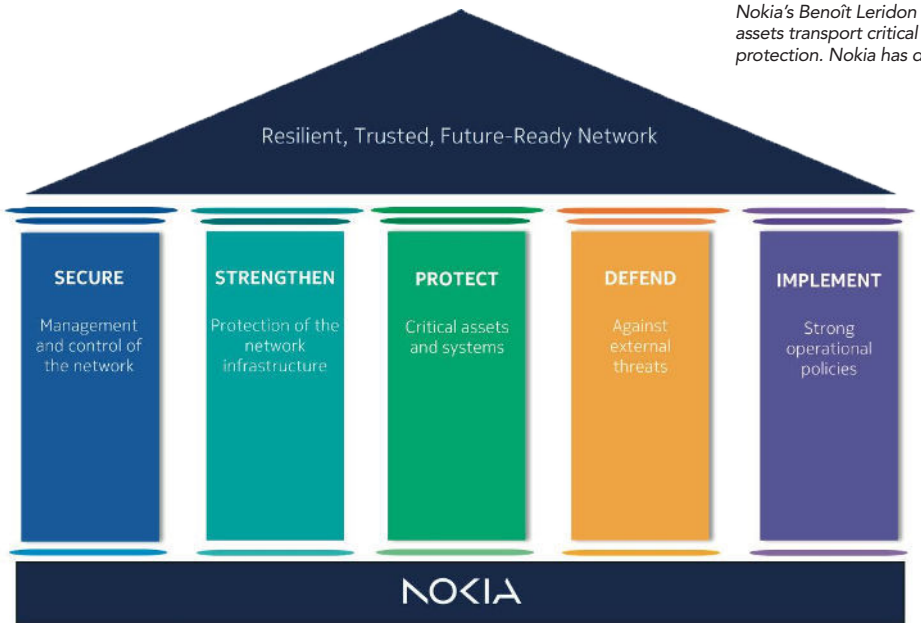
The topic of cyber threats against smart rail is anything but hypothetical. "Several incidents stand out for what they reveal about where the real risks lie," Shifman said. "In 2022, the hacktivist group Cyber Partisans targeted railway systems in Belarus, encrypting a large portion of servers, databases, and workstations in protest of Russian troop movements through the country. Train operations were forced into manual mode. Notably, the attackers stated they deliberately avoided causing unsafe conditions, demonstrating a level of intent and control that is uncommon in hacktivist activity."

Also in 2022, a ransomware attack on a Danish railway's IT subcontractor compromised the system it used to receive speed restrictions and track status updates. As a safety precaution, railway operations were halted.

"During the same period, railway systems in Ukraine were targeted by a cyberattack attributed to Russian intelligence, which took online ticketing offline for 89 hours during the early stages of the invasion," said Shifman. "In Italy, a ransomware attack disrupted ticketing machines at stations nationwide."

The Risks of Relying on IP

Modern railways rely on IP-based networks to interconnect signaling, interlocking, train control, maintenance, and traffic management systems. "This convergence means a traditional network intrusion can propagate across domains



Nokia's Benoît Leridon says railways are unique because their deployed telecom assets transport critical applications in locations where there is little or no protection. Nokia has developed their security pillars shown here.

that directly influence train movement or availability. Interconnectivity introduces systemic risk: a failure or manipulation in one subsystem can cascade, creating service paralysis or forcing emergency operational modes," Thesee said. "The risk is not hypothetical — automation amplifies impact because decisions are executed at machine speed, leaving little margin for human intervention."

Unfortunately, IP-based networks provide a much broader attack surface than the serial communication systems they replaced. This is because many rail protocols that originated in serial point-to-point communications were migrated to IP for interoperability and cost reasons, while lacking the security architecture that IP environments require. "These protocols carry no authentication or encryption by design," said Shifman. "They were conceived for isolated, closed networks where trust was assumed. So, when those protocols run over IP, they become reachable. An attacker who enters the network through any connected system has potential access to control communications that were never designed to be exposed."

How to Fight Cyber Threats

Smart railways that take cybersecurity seriously take steps to minimize the risk of intrusions into their systems, and to minimize the impact of any intrusion that does occur. "If the measures are well implemented, only a highly sophisticated attack can penetrate them," Leridon said. "That is where firewalls and XDR systems come into play to block attacks."

Short for Extended Detection and Response, XDR is an advanced cybersecurity platform that brings together security data from across an organization's entire digital environment, including endpoints, networks, and cloud services. By using AI to analyze this data, XDR can automatically detect, investigate, and neutralize sophisticated cyber threats that might slip past traditional security tools.

Multiprotocol Label Switching (MPLS) is another way in which smart railways can contain cyber threats. MPLS does this by creating a system of isolated digital highways within a smart railway's IP infrastructure. This isolation separates critical train control systems from vulnerable networks like public Wi-Fi. In this way, MPLS guards against network flooding attacks by strictly prioritizing life-safety data, thus shielding a railway's internal network structure from external attackers. However, because MPLS does not encrypt data itself, this system must be protected by encryption protocols, firewalls, and XDR systems.

"MPLS networks are built according to IEC 62443 with a native implementation of zoning, which controls traffic and thereby limits risk," said Leridon. (IEC 62443 is a globally recognized cybersecurity standard designed to protect critical industrial automation and operational technology (OT) — such as a smart railway's physical train control and signaling systems — from cyberattacks.) "This technical foundation is complemented by a zero-trust approach provided by the network. Then, XDR with AI may be applied to enhance protection for the most critical applications."

AI and its subset, machine learning (ML), are playing a vital part in fighting cyber threats. AI is not being used as an autonomous "defender" fighting threats on its own, "but as a decision-support layer enhancing anomaly detection in complex railway environments," Thesee told TSI. "AI-assisted monitoring is being used to correlate deviations in network traffic, system behavior, and operational baselines that human operators cannot detect in real time. But AI introduces new trust dependencies: data poisoning or model manipulation could undermine detection itself. Therefore, AI deployment in rail security is framed as augmenting human-led SOC operations, not replacing them."

On a narrower scope, Cylus' CylusOne uses machine learning algorithms to detect anomalies in signaling and control networks. "The baseline we build is not a generic IT baseline. It accounts for rail operational context: shift patterns, train schedules, maintenance windows, and the expected communication patterns between specific OT components," said Shifman. "What this means in practice: An unusual command sent to an interlocking at 2 a.m. during a maintenance window might be expected. The same command sent mid-service day with no corresponding maintenance record is flagged immediately. The system also generates AI-driven descriptions of every alert in plain language, with rail-specific context and recommended mitigations, so that operators without

deep cybersecurity backgrounds can act on them."

When cyberattacks do disrupt smart railway operations, satellite-based positioning systems like GPS step in as traffic management tools. "The value is resilience," Shifman said. "When ground-based network connectivity fails, satellite positioning can maintain situational awareness of where trains are."

"When centralized traffic management or communication networks are degraded, independent positioning sources can help maintain situational awareness and separation logic at degraded but safe operational levels," agreed Thesee. But "these systems must themselves be protected against spoofing and jamming, reinforcing a broader point: resilience is about layered diversity, not single-technology trust."

Protecting Against The Quantum Threat

Hackers are now using AI to create cyber threats that are vastly more sophisticated and harder to detect. When quantum computing finally arrives — a level of computational power that will dwarf what is currently being used — hackers will be able to crack the most complex of current encryption algorithms. In the meantime, many are stealing encrypted data and storing it for the day that quantum computing can help them crack it. These are known as "harvest now, decrypt later" (HNDL) attacks.

In response to this threat, many smart railways are pursuing "quantum-safe encryption" to protect themselves against quantum-enabled attacks. "While quantum-safe cryptography is not yet universally deployed, operators and suppliers are already required to plan cryptographic agility into architectures so that algorithms can be replaced during decades-long operation," said Thesee. "This is not speculative security, but lifecycle responsibility, now reinforced by regulation."

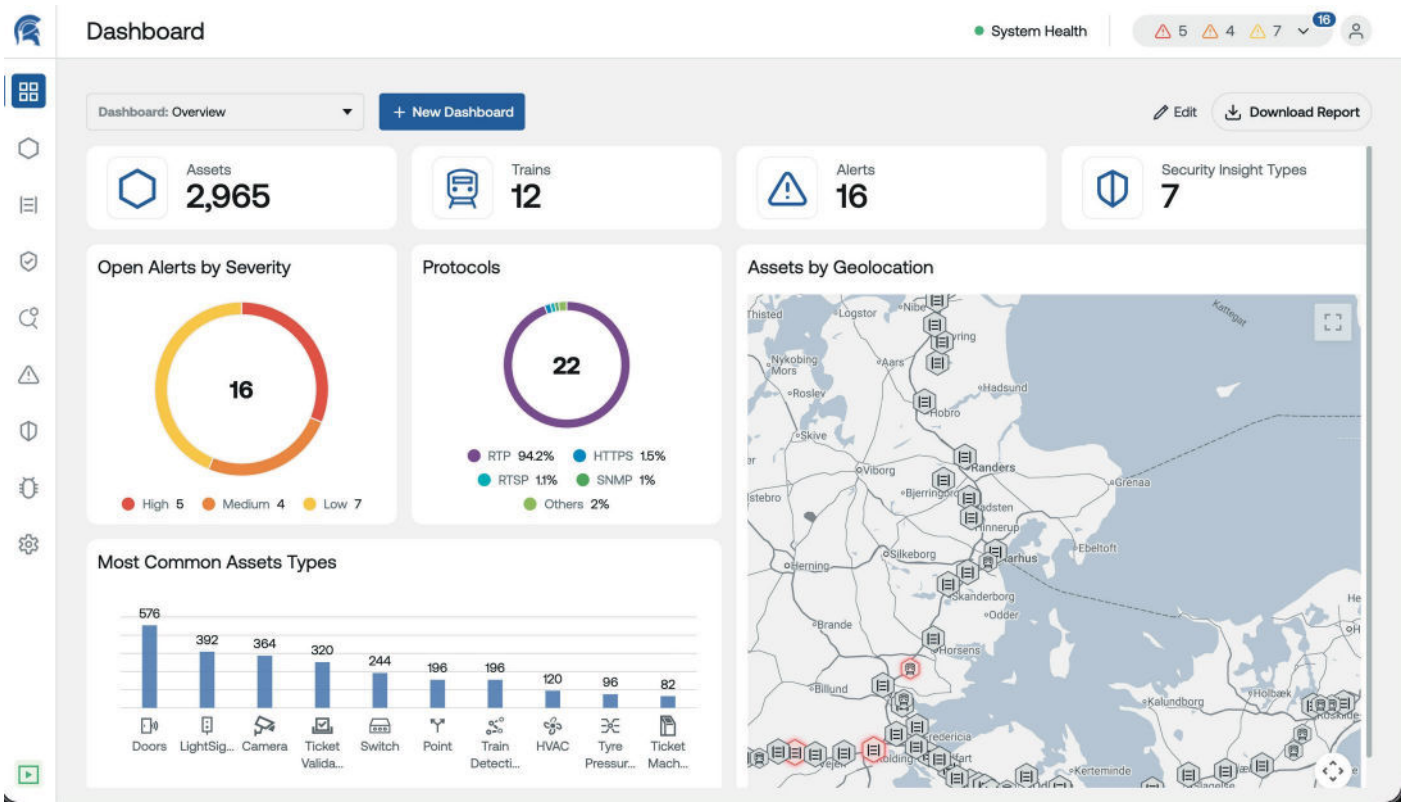
"There's no certainty that harvest-now, decrypt-later attacks currently apply to rail," Leridon noted. "However, infrastructure managers are applying quantum-safe encryption. And in recent years, they have required network equipment with MACsec, which is a crucial foundation of quantum-safe networking."

Short for Media Access Control Security, MACsec is the IEEE 802.1AE network security protocol that encrypts data ... If MPLS provides the dedicated "highways" for separating railway data, MACsec is the armored convoy that travels on that road.

There's another reason that smart railways need to deploy quantum-safe encryption, namely "active spoofing." "Quantum computers capable of breaking today's asymmetric encryption would allow an attacker not just to read protected communications, but to forge them," said Shifman. "In a rail context, that means injecting digitally signed commands that safety systems accept as legitimate. Movement authority, interlocking states, train control messages — if the authentication protecting those signals can be broken, an attacker can send instructions the system will trust and act on. That is a direct safety threat, not just a data confidentiality issue."

At present, most smart railway

Cylus' CylusOne uses machine learning algorithms to detect anomalies in signaling and control networks. Cylus image.



operators have not started their migration to quantum-safe cryptography. "The challenge is compounded by the infrastructure lifecycle: assets installed today may still be operational when quantum capabilities mature," Shifman said. "The groundwork that needs to start now is identifying which systems rely on public-key cryptography to authenticate safety-relevant communications, and beginning the transition planning before the window closes."

The bottom line: "Rail operators are now considering security as an end-to-end, in-depth strategy, rather than using a highly centralized approach," said Leridon. "Because threats can come from everywhere, each network has to be protected everywhere. That's why a zero-trust approach (where users and devices face repeated authentication challenges as they move through the network) is being considered far more widely."

How Regulations Are Improving Cyber Security

No one likes regulations. However, they are useful tools for improving cyber security in the railway sector, at a time when such improvements are much needed.

A case in point: In the U.S., TSA's security directives for rail have moved the industry from voluntary guidance to enforceable requirements. "The first generation, issued in late 2021, required operators to designate a Cybersecurity Coordinator available 24/7, report incidents to CISA within defined timeframes, conduct a vulnerability assessment, and develop a Cybersecurity Incident Response Plan," Shifman said. "The second generation, issued in 2022 and updated since, is performance-based and more substantive. Operators must submit a Cybersecurity Implementation Plan to TSA covering five outcomes: network segmentation between IT and OT, access controls including multi-factor authentication and least-privilege principles, continuous monitoring and anomaly detection, and structured patch management. An annual Cybersecurity Assessment Plan is also required, ensuring the full scope of measures is independently tested on a rolling three-year cycle."

In Europe, NIS2 and the rail-specific standards CENELEC TS 50701 and its future global version, IEC 63452, are creating equivalent baseline expectations, extending requirements across the supply chain to include integrators and vendors, not just operators. Additionally, "the EU Cyber Resilience Act (CRA) and NIS2 transform cybersecurity from 'best effort' into mandatory, auditable obligations," said Thesee. "Products with digital elements — including signaling and train control — must demonstrate secure-by-design practices, vulnerability handling, and long-term patch support. This regulatory pressure is a structural driver for modernization, compelling alignment between safety certification and cybersecurity lifecycle management."

Overall, "what has fundamentally changed is accountability," Shifman said. "Cybersecurity has moved from a risk management decision that operators could defer to a compliance requirement with defined controls, reporting obligations, and regulatory oversight."

The Challenges of Centralizing Security

Ideally, modern railway Security Operations Centers (SOCs) should be capable of monitoring both traditional IT and physical OT in real time. So what are the challenges standing in the way of this goal?

"The core challenge is that IT and OT speak different languages, technically and operationally," replied Shifman. "A SOC analyst trained in IT security works with network logs, SIEM (Security Information and Event Management) alerts, and endpoint telemetry. Rail OT produces entirely different signals: protocol-level events in CBTC (Communications-Based Train Control) or ERTMS (European Rail Traffic Management System) communications, configuration changes in interlocking systems, anomalies in train movement data. Generic SIEM tools can ingest this if the data is translated, but without rail-specific context, analysts have no baseline for what normal looks like."

The second hurdle in creating an integrated rail SOC is what Shifman calls the "operational constraint on response." "In IT, isolating a suspected system or blocking traffic is a standard first action," he explained. "In rail OT, you cannot isolate a signaling component during service hours without operational consequences. Every response procedure has to be evaluated against safety and availability. SOC playbooks built for enterprise IT will cause problems if applied to rail OT without adaptation."

The third is staffing. "Rail cybersecurity expertise is rare, and analysts who understand both IP networking and interlocking logic are genuinely hard to find," said Shifman. "The practical path operators can take is tooling that translates rail OT events into SOC-consumable alerts with enough operational context that analysts can triage effectively without deep rail domain knowledge."

This being said, "the main hurdles are organizational and architectural, not technological," Thesee observed. "Talent, process integration, and trust between engineering and security teams are the real bottlenecks, because implementing an efficient rail SOC requires a deep integration of railway knowledge with cybersecurity expertise," Thesee observed. "Without mastering IT, OT, and railway operations, the SOC will not deliver the expected value."

The Smart Railway Report Card

Now that we've enumerated the cyber risks facing smart railways, one last question remains. How well are the railways addressing these threats?

From Alstom's perspective, "Our current assessment on this topic is balanced," said Thesee. "The rail industry has made significant progress through standards (IEC 62443 or IEC63452), regulation and growing awareness. However, gaps remain in legacy system hardening, supply-chain transparency and operational cyber-resilience testing."

Shifman echoed Thesee's balanced assessment. "The industry is improving, and the shift happening now is foundational," he said. "Rail operators are establishing OT monitoring programs at a pace we haven't seen before,

The rail industry has made progress, but gaps remain in legacy system hardening, supply-chain transparency and operational cyber-resilience testing, according to Alstom's Eddy Thesee. Alstom image.

driven by a growing understanding of a simple principle: you cannot protect what you cannot see. For years, rail OT environments were largely invisible from a security standpoint. Operators knew their systems existed, but lacked clarity on communications, exposures, and what 'normal' behavior looked like. Building that visibility is the critical first step, and more operators are now taking it seriously."

Having said that, Shifman warned that visibility alone is not enough. "Context is everything," he told TSI. "Alerts without operational context quickly become noise. To be effective, security tools and SOC teams must understand rail operations, not just cybersecurity, in order to distinguish between expected behavior and real threats. The industry is starting to build this capability, but it remains uneven."

On a broader scale, what needs to be done is to translate this visibility into action. "This means integrating security into operational processes, prioritizing risks based on real-world impact, and enabling faster, more confident responses," said Shifman. "It also requires deeper collaboration between IT, OT, and engineering teams, as well as solutions tailored specifically to rail environments rather than adapted from generic IT security. Until security becomes part of day-to-day railway operations, not just a monitoring function, the gap between detection and effective mitigation will remain."

Asked for his assessment, Leridon said that end-to-end communications security must be established by smart railways, ahead of any other protective steps. "Railway networks must rely on highly complex telecom networks, due to their spread, their lifecycles, their regulatory constraints, and the critical nature of the applications they control," he said. "The first essential step is to ensure that the network is protected from everywhere — and that a zero-trust approach is applied. Without this first building block, even sophisticated tools such as IDS, Firewalls, XDR, will proliferate with no real benefit to security."

The takeaway: "Cybersecurity in rail is no longer optional," concluded Thesee. "But it is still uneven, and resilience — not just prevention — must become the defining metric."