NOKIA

Securing digital railways against cyber-attacks

A growing array of cyber-security challenges

The adoption of IP-based networks and Internet of Things (IoT) technologies is enhancing safety, increasing operational efficiency and improving the passenger experience. Yet, because these networks are more interconnected than traditional railway communications systems (which tend to be more isolated), they can increase the vulnerability of railway operations to cyber-attack.

Similarly, the growing use of sensors, meters, surveillance cameras and other devices to support real-time monitoring opens the possibility of IoT devices providing a back door into the network. Railways are also taking greater advantage of wireless networks from GSM-R to LTE to 5G technologies that must be engineered precisely to ensure full security.

Threats arise in many ways, not just from criminals, foreign agents, or even disenchanted employees. Many breaches can be traced back to human error and even the best trained staff can be overwhelmed by the sheer volume of daily attacks.

Railway operators also face increasingly stringent legal, regulatory and compliance requirements, making them directly accountable for ensuring effective information security.

A robust, end-to-end cyber-security strategy can address many of these challenges.

Defense in depth

Nokia offers in-depth expertise on cyber-security best practices. We work with you to ascertain the underlying risks to your network. Developing an airtight, secure network would require an unrealistic level of investment. Nokia instead advocates defense in depth as a more balanced, economically feasible approach to security that mitigates the real risks.

We build cyber-defenses aligned with a network's operational objectives to achieve layered security across network, application, data, identity and access management, establishing a series of defenses that close off any attempts to exploit security gaps. Nokia end-to-end security solutions encompass business processes, regulations and security policies to keep pace with the rapid rise in attacks.

Network element -based security

Nokia combines expertise in both wireless and IP to achieve mission-critical security that addresses the vulnerabilities specific to these technologies. Mission-critical network solutions (IP/MPLS, optical, GSM-R, 5G) not only deliver network reliability, performance and scalability, they also defend against security threats and attacks.

SOARing to secure operations

Nokia employs the security orchestration, automatization and response (SOAR) model, introduced by Gartner, to provide the tracking and analysis capabilities railways need. Nokia's SOAR solution, NetGuard Security Management, can interact with technologies from a variety of providers that collect data and/or trigger specific actions.

Smarter security systems

Through the application of advanced analytics and machine learning techniques, NetGuard Security Management can provide complex correlation and detection capabilities for precise security risk prediction, faster root cause analysis, faster response times through the application of pre-defined rule books and simplified (and standardized) reporting to federal and/or regional security incident response teams.

Empowering security teams with automation

Customizable dashboards with powerful search and reporting capabilities can be optimized for the individual needs of security management teams. Automated workflows facilitate the investigation and mitigation of threat incidents, enabling experts to accelerate their response.

How you benefit

- **Improved railway safety and operational efficiency**
  Effective cyber-security enables the safe adoption of new IP-based applications for train control, signal control, maintenance monitoring, video protection and passenger information systems.
- **Protection against financial damage**
  Security incidents can be costly, not just in terms of the loss of revenue from disrupted passenger services, but the recovery and restoration costs, potential lawsuits, damage to brand reputation, compensation to users and non-compliance penalties. Defense in depth can reduce these risks.
- **Ensuring security compliance**
  Meet the increasingly stringent legal, regulatory and compliance requirements through more effective information security and data privacy.
- **Focusing on running rail operations**
  End-to-end Nokia security enables you to focus on your mission-critical responsibilities without being distracted by the daily operation of a telecom business or by having to work with multiple security vendors.

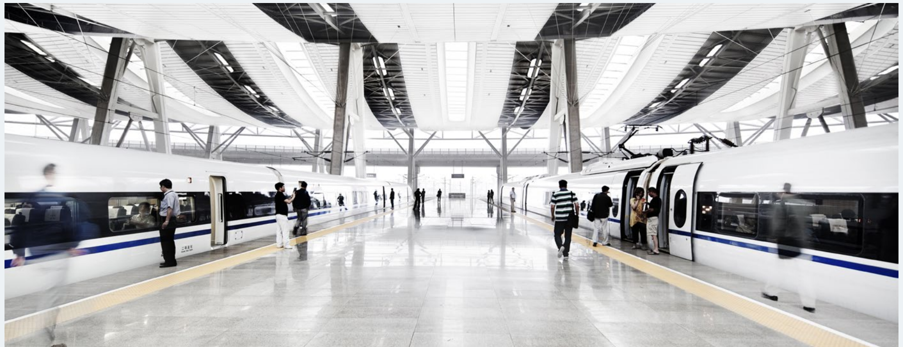
Case study

Nokia is providing an in-depth cyber-security solution as part of network modernization for large, state-owned European railway. To counter increasingly pervasive threats from cyber-attack as well as human error such as configuration problems and non-compliance with security protocols. The Railway is adopting a multi-tiered approach, built around the following products:

- The Nokia NetGuard Identity Access Manager (IAM), which secures physical and virtual network functions and resources, providing unified identify access control, single sign-on with centralized policy management and advanced access management to minimize unauthorized incursions.
- The Nokia NetGuard Virtual Firewall (VFW), which support segmentation of different applications on the network, helping to isolate and limit the impact of attacks.

Employing a comprehensive, in-depth cyber-security regime will enable the Railway to adopt new IP-based applications for a variety of critical functions (train control, signal control, maintenance monitoring, video protection and passenger information systems) safely and securely. The Railway's new cyber-security architecture will help eliminate or quickly mitigate threats, allowing it to focus on its primary operations, delivering people quickly and safely to their destinations.

For more information on Nokia cybersecurity solutions for railway operations, click here



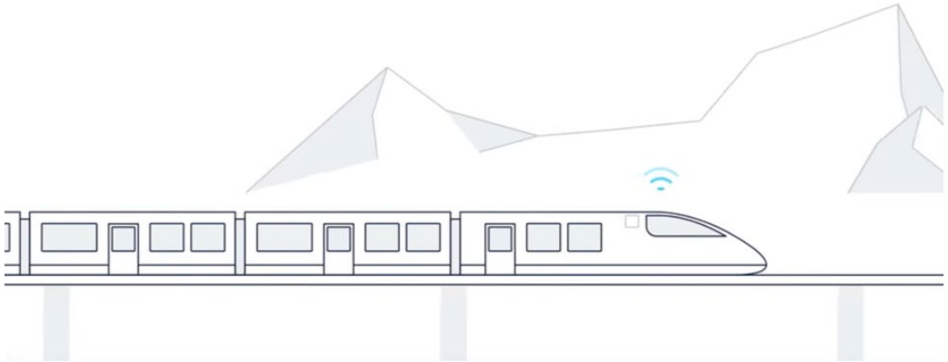
How in-depth security changes the game

- **Automation meets the avalanche of threats**
  Automating incident response ensures defenses are not overwhelmed by thousands of daily alerts.
- **End-to-end security protects all network technologies**
  End-to-end security encompasses the entire network and its security processes, such as: access management and audit compliance; network security; and security management for IoT devices.
- **Network segmentation and firewall confine threats**
  Network segmentation with IP/MPLS VPN provides traffic isolation and hampers lateral movement of hackers as they scout the network.
- **Analytics for continuous improvement**
  Security analytics correlates data from across the network, devices and cloud layers to spot and characterize suspicious anomalies, along with the associated business risk and recommended response; applying machine learning increases effectiveness over time.
- **Encryption protects data**
  Multi-layer encryption ensures that even when a perpetrator taps into the communication channels, confidentiality, integrity and authenticity are still secure.
- **High availability and operational stability**
  Network and transport layers enable rapid recovery from any attack, including physical shut down of communications equipment and infrastructure facilities.

Why Nokia?

- More than 30 years' experience in the rail industry
- Expertise in working with rail operators to developing proactive security strategies
- Leverages strong presence in the public safety segment, and as a trusted partner for public network operators around the world
- Offers a comprehensive approach built on its in-depth experience and expertise in both security and mission-critical networks and operations
- Mission-critical networking portfolio (IP/MPLS, optical, and wireless) features strong, built-in security mechanisms augmented by the NetGuard portfolio's end-to-end security architecture
- Provides the right balance of costs with the in-depth protection needed to defend railways against today's security threats

Want to learn more about cyber security for railways? **Get the white paper**



Nokia Oyj
Karaportti 3
02610 Espoo
Finland

nokia.com/networks/topics/cyber-security-railways

Document code: SR1907036680EN (September) CID: 206596

About Nokia
We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience.
www.nokia.com