NOKIA

Cyber security for railways

White paper

Digital transformation is bringing substantial benefits in railway safety, operational efficiency and reliability, as well as an enhanced passenger experience. Yet, it also inevitably increases the vulnerability of railways to cyber-threats.

This means that the continued protection of rail infrastructure will require stronger and more robust railway communications network security, with new technological and process measures being implemented.

Contents

1. Executive summary

The consequences of a successful major cyber-attack on a nation's rail infrastructure could be catastrophic. A metro transport system brought to a standstill for even a short period would cause city wide havoc, damaging the local economy, harming the metro operator's bottom line, and making passengers doubtful about the future safety and reliability of transport services. Worse, a successful attack on a communications-based train control system could cause an accident, putting lives at risk.

Nobody in the industry wants any of that to happen. Yet, based on Nokia's experience in the industry, the risks of cyber-attacks occurring are often underestimated by rail operators.

In a July 2017 speech, Suresh Prabhu, Indian Railway Minister summed up the need for better security in railways: "When we do everything manually, the challenge is manual error and if we are shifting from manual to technology-oriented operations, then the flaws in technology, or someone who can potentially hoodwink it, is as high and sometimes even more dangerous. So cyber-security is one of the top priorities."[1]

Unfortunately, some attacks have succeeded in the past, resulting in serious consequences in several countries.

Digital transformation in railway operations has ushered in new applications to monitor and control rail systems. These applications are typically based on IP technologies, generating a wide range of IP traffic flowing across the communications network. Examples of how digitization is being deployed more widely include train control, control of signaling, maintenance monitoring, video protection and passenger information systems.

Cyber-attacks are a growing threat to all types of mission-critical networks, including those used by railways. Security agencies recognize the risks. In the US, cyber-security is seen as a serious economic and national threat with the US Computer Emergency Readiness Team (US-CERT) creating a framework to support the protection of critical infrastructure. In Europe, the EU has proposed a cyber-security strategy outlining its vision, clarifying roles and responsibilities, and defining actions required to protect citizens.[2] In Asia, some governments have established national cyber-security policies.

Consequently, railway security must be stepped up. Railway operators should consider implementing a security life cycle strategy by applying technical solutions and enhanced security practices/processes.

To keep pace with the rapid rise in attacks, operators should consider shifting from legacy reactive security infrastructures (detection and response) into proactive automated security life cycles. Key capabilities to protect networks must include security automation that encompasses business processes, incident response plans, regulations and policies; end-to-end security that encompasses the operation of the network and its processes; security analytics to correlate security-related information from across the network, devices and cloud layers to spot suspicious anomalies and provide insight into threats; and multi-layer encryption to protect network traffic.

Such a multi-layered and active security approach provides the right balance of costs with the in-depth protection needed to defend against today's security threats, while ensuring that railway operators are prepared to meet their compliance obligations.

[1] http://www.ehackingnews.com/2017/07/railways-to-focus-on-cyber-security.html

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

2. Railway infrastructure is under attack

Cyber-attacks have become a global phenomenon. Several relatively recent incidents have shown how a successful cyber-attack can cause mayhem for railways. In one high-profile case in 2003, a virus infection of a train company's systems in Florida disrupted signaling, dispatching and other systems, resulting in widespread delays across the eastern US.[3]

In 2008, a 14-year old managed to hack systems in the city of Lodz in Poland, causing tram derailments and passenger injuries.[4]

In 2016, it was widely reported that UK railway infrastructure was the victim of at least four major cyber-attacks in the previous year.[5]

In 2017, the widely publicized Wannacry[6] attack affected many organizations globally. Germany's Deutsche Bahn rail infrastructure suffered system failures and ransomware messages appearing on station information screens.[7]

Security incidents like these cost railway operators in many ways. Not just the loss of revenue while services are unavailable, but the recovery and restoration costs, potential lawsuits, damage to brand reputation, compensation to users and non-compliance penalties.

> "Railway systems are becoming vulnerable to cyber-attack due to the move away from bespoke stand-alone systems to open-platform, standardized equipment built using Commercial Off The Shelf (COTS) components, and increasing use of networked control and automation systems that can be accessed remotely via public and private (communications) networks."
>
> Rail Cyber Security, Guidance to Industry, Department for Transport, UK, February 2016[8]

[3] http://www.cbsnews.com/news/virus-disrupts-train-signals/

[4] http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

[5] http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attackslast-year/

[6] https://www.us-cert.gov/ncas/alerts/TA17-132A

[7] http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackerstarget-deutsche/

[8] https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cybersecurity-guidance-to-industry.pdf

3. Rising regulatory and data privacy pressure

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

In Europe, the EU cyber-security strategy[9] lays out roles, responsibilities and defines actions required to protect citizens. In fact, failing to prepare adequately to address cyber-security threats is a substantial risk in and of itself.

For instance, regulations such as the European Union's Network and Information Security (NIS) directive demand that comprehensive protections be put in place, and failure to do so can result in substantial penalties. While the interpretation of NIS can vary from country to country, certain fundamental standards need to be met and maintained. It is clear that any successful plan will depend on the ability to detect risks (in advance) and mitigate threats, whether from hostile actors or simple human error. Real-time monitoring and reporting capabilities are a baseline requirement to enable security teams to track and respond to emerging events. Operators will need to monitor and report compliance to minimum security requirements, proactively assess the potential business impact of a breach and report security breaches.

Solutions are now available that follow the security orchestration, automatization and response (SOAR) model, introduced by Gartner to provide the needed tracking and analysis capabilities. These solutions can deliver a variety of benefits, notably the elimination of unauthorized access and misconfiguration, 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.

In addition, maintaining privacy standards and protecting citizens' data is an increasing priority in many jurisdictions. The General Data Protection Regulation (GDPR) rules in Europe, for instance, tighten data privacy requirements substantially.

Regulators are also specifying minimal compliance requirements for privacy protection that are verifiable before a communications element can be used in the telecom network of any carrier. To safeguard the privacy of their citizens, some governments are proposing legislation requiring their citizens' data be stored within the boundaries of their country and governed by their privacy laws.

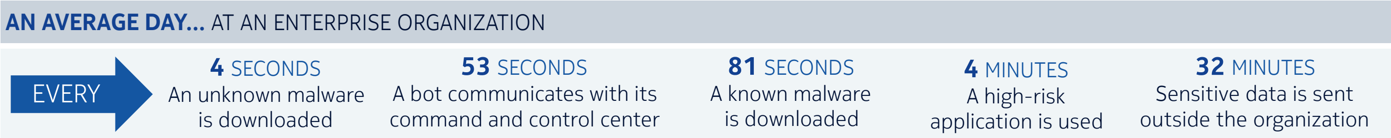
4. Successful attacks on critical infrastructure provide valuable lessons for railways

Incidents in Ukraine have created some insight into how cyber-attacks unfold. In December 2015, a major attack was launched on power grids in the Ukraine, leaving 250,000 people without electricity. Almost exactly a year later, hackers struck again and parts of Kiev suffered a power outage lasting about an hour.

The 2016 attack is said to have been caused by sophisticated new malware that could automate attacks on other mission-critical networks around the world.[10] The lesson is clear - cyber-attacks can disrupt mission-critical services and put lives at risk.

[9] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[10] https://www.wired.com/story/crash-override-malware/



AN AVERAGE DAY... AT AN ENTERPRISE ORGANIZATION

EVERY	**4** SECONDS	**53** SECONDS	**81** SECONDS	**4** MINUTES	**32** MINUTES
	An unknown malware is downloaded	A bot communicates with its command and control center	A known malware is downloaded	A high-risk application is used	Sensitive data is sent outside the organization

Figure 1. Enterprises face constant threats from malicious software every day.[11]

Anatomy of an attack ... and how to prevent it

Stage 1: Break-in

The Ukrainian power system attack in 2015 began in June 2014 when hackers targeted administrative and other personnel in the power company through a campaign of phishing emails with attached documents that enabled macros to install malware.

Stopping the threat: Deploying endpoint security would detect command-and-control traffic, before malware is detonated.

Stage 2: Expand and prepare

The hackers were then able to harvest credentials and gain privileges throughout the IT system. The task was made easier because passwords were hard-coded and shared passwords were not changed regularly. The hackers set up an IPSec virtual private network (VPN) connection direct into the network.

Stopping the threat: Deploying credential protection to provide a secure point of control. Implement anomaly protection to detect suspicious behavior. Using IP/MPLS VPN and a firewall to impede and restrict the hackers' lateral movement.

Stage 3: The attack

After about six months of undetected preparation, the hackers executed the attack, disconnecting circuit breakers and hindering recovery through a DDoS attack on the call center, blocking and wiping workstations, servers and endpoints. They also installed firmware to block remote commands. Recovery required physical visits to each substation to manually reset circuit breakers.

Stopping the threat: Deploy automated response solutions that can respond to threats before they become breaches.

[11] http://www.internetworking.ch/files/eng-checkpoint-2015-securityreport.pdf

5. The risks are everywhere … and many-sided

Highly sophisticated attacks are likely to require the backing of a state, large terrorist group or sophisticated criminal organization. Such groups share similar goals: to disrupt operations or even steal information to gain a financial or strategic benefit. The motivation for groups to target rail communications networks can range from a pure demonstration of force to simply gaining publicity, venting grievances, or making a political statement.

Yet these are not the only perpetrators. Up to 70 percent of security incidents are the result of some form of insider attack or simple human error. For instance, disgruntled employees may use their privileged access rights to alter security configurations. Such failures open operators up to many different types of attack. They include data theft and tampering, eavesdropping and potentially damaging distributed denial of service (DDoS) attacks. There is also a fast-growing and potentially far more damaging category of attack known as a destruction of service (DeOS) attack that can physically damage hardware and equipment by, for example, corrupting the firmware on internet connected devices.

Fairly simple mistakes that enable IDs to be stolen through phishing attacks or more routine security breaches such as the use of weak or stale passwords can put systems at risk. Eliminating these security holes is critical and requires robust and consistent security policies coupled with automated, network-wide security measures such as password aging and complex password requirements.

Security can also be improved through the use of standardized, unified access security policies across the network infrastructure, such as the implementation of identity management systems for privileged users of critical networks, including comprehensive video/text logging to help ensure a high compliance to key security specifications. This helps address a growing need on the part of railway operators to better track who has accessed the network, and when, to enable them to identify the source of vulnerabilities and ideally who used the resulting back door. This long term forensics capability is often also required by regulators.

5.1. IP and IoT increase the risks

The evolution of railway communications networks to IP technologies and the increasing use of IP-based applications and the growing adoption of Internet of Things (IoT) technologies are widening the spectrum of vulnerability of rail infrastructure.

In the past, systems tended to be isolated, providing natural breaks that could stop the spread of a malicious infection or the reach of an attack. However, today's IP-based applications and underlying mission-critical networks are more interconnected, increasing their vulnerability.

The need to run new IP networks alongside legacy technologies, such as SCADA, adds further security complexity. A good example of how legacy vulnerabilities can carry forward into today's systems is Signaling System No. 7, or SS7, which was designed more than 40 years ago. The underlying methodologies for the SS7 signaling protocol, as used in GSM/GSM-R for example, have been incorporated into Diameter, a protocol used in standard IT-based, packet-switched/Ethernet-based solutions, including LTE wireless networks. As a result, security threats to SS7 networks may also be possible in LTE networks, requiring increased security on signaling interconnects.

Another potential security threat might arise from the forthcoming deployment of ETCS (European Train Control System) over GPRS/IP.

Meanwhile, the growing use of sensors, meters, surveillance cameras and other devices to support realtime monitoring and situational awareness, improves operational efficiency, reliability, resiliency and safety of railway infrastructure.

This evolution is bringing about the risk of cyber-attackers gaining control of IoT devices and using them to run malware to engage in attacks ranging from spam to data theft to DDoS.

Indeed, it is possible, even likely, that there are many installed devices today that have been compromised, yet their infection is undetected because they continue to perform their intended functions. A hacked sensor could be sending millions of spam messages per month over a long period of time, but this may not be obvious unless the IP address range is blacklisted. However, state-of-the-art IoT security solutions can monitor the network traffic generated by the IoT devices and alert for abnormal behaviors, which can go a long way toward helping railway operators address this challenge.

For devices that are part of a mission-critical application, such as signaling, alerts or faults must be processed in real time to ensure seamless service continuity. Just as important, corrective actions must be initiated automatically, either from or to the IoT devices, based on security policies. Finally, the data transmitted to and from IoT devices needs to be auditable to enable accuracy, governance, and regulatory compliance.

In October 2016, attackers managed to hack 145,000 IoT devices to execute the world's first terabit scale distributed denial of service (DDoS) attack[12]. The attack, using a weapon called the Mirai botnet, affected a wide range of organizations from Paypal to Twitter, to Amazon to Spotify. In March 2018 and January 2019, there were even larger volumetric DDoS attacks, of 1.3 terabits per second and 580 million packets per second respectively, trying to oversaturate the network capacity as well as server processing power while denying legitimate requests and transactions. While such attacks have not yet directly target mission-critical networks it does show how IoT devices like smart sensors and cameras can be manipulated to bring operations to a complete halt.

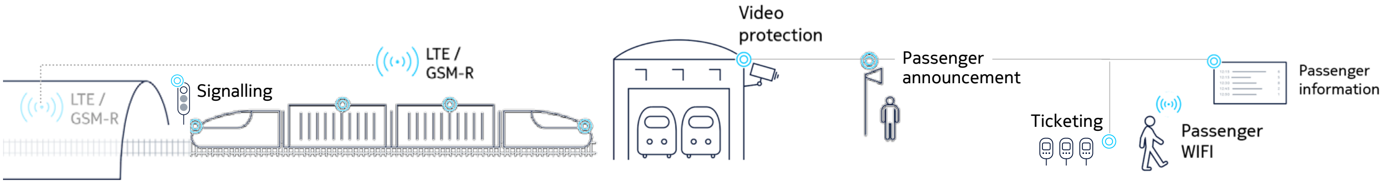


Figure 2. The evolution to interconnected IP-based systems plus the rise in the use of internet-connected devices increases the vulnerability of railway operators to cyber attack.

5.2. IP-based wireless networks need extra protection

A further development is the adoption by railways of wireless networks in the form of LTE and future 5G technologies. LTE security is based on two layers of protection instead of one-layer perimeter security as in 3G. The first layer deals with security in the radio access network, while the second layer provides security in the Evolved Packet Core (EPC) network. In practice, the implementation of this two-layer security architecture is subject to vendors' interpretation and therefore, may expose a mission-critical network to threats if not engineered properly.

The encryption of all traffic between base station and core network is also essential. LTE networks provide hop-by-hop protection that could lead to security being compromised by incorrect system configuration parameters. End-to-end encryption provides protection for situations where security is not configured properly in LTE equipment.

[12] https://www.siliconrepublic.com/machines/internet-meltdown-mirai-botnet

In railway networks, voice services depend on group communications in which users can simultaneously communicate, walkie-talkie style, with groups of other users. These require specific arrangements to secure group call communication and direct mode of operation, as well as ensuring the security of both device and back end control servers.

6. Defense-in-depth is vital to protect railway operations

Cost-effectively protecting railway networks from cyber-attacks first requires an understanding of the risks to the specific networks and their underlying operational processes to define the scope and appropriate level of protection required. Even if a completely airtight, secure network would be possible, it would require an unrealistic level of investment. Rather, defense in depth is a more balanced, economically feasible approach to provide the necessary security to mitigate the real risks.

The objective is to build cyber-defenses that are aligned with the network's operational objectives. Railway operators must focus on processes and technologies to implement effective layered security across network, application, data, identity and access management, laying out a series of defenses to thwart attacker's attempts to exploit security gaps.

Humans also play a predominant role in cyber-defense. Supplementing all security measures in place, rail operators need to train all employees to be prudent in electronic communications and be vigilant about reporting any anomalies, reducing security risks and protecting the rail systems.

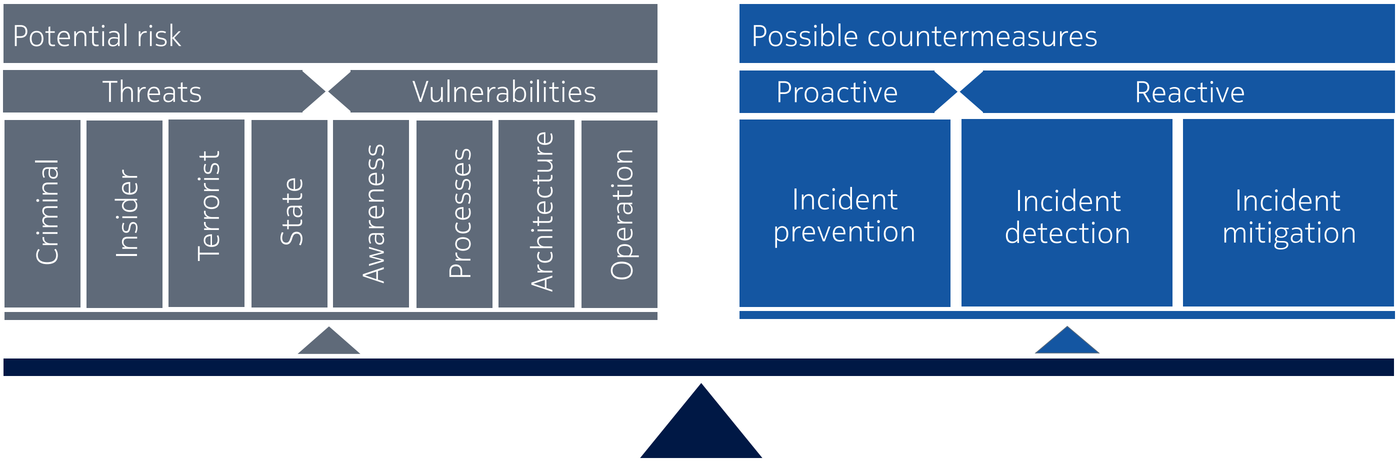


Figure 3. Security always requires a balance between the risk from threats/vulnerabilities and required investments for countermeasures.

6.1. Security is everybody's responsibility

Technical solutions that help to protect infrastructure need to be accompanied by processes and management procedures that instill a culture of security in all railway employees.

The point is made clear by the UK's Department for Transport in its publication Rail Cyber Security Guidance to Industry:8 "When implementing security there is a natural tendency to focus the majority of effort on the technological elements. Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice."

The internet carries many examples of how even the most basic of security recommendations are not being followed – such as revealing log-in details. In the UK, a 2015 TV documentary revealed how one railway operations center employee had written down username and password details on a monitor.[13]

It also reveals the use of weak passwords, as does another filmed TV interview in which a Polish organization's password information was clearly displayed on a whiteboard.[14]

Eliminating this security hole is critical and requires robust and consistent security policies coupled with automated, network-wide security measures such as password aging and complex password requirements.

Security can also be improved through the use of standardized, unified access security policies across the network infrastructure, such as the implementation of identity management systems for privileged users of critical networks, including comprehensive video/text logging to help ensure a high compliance to key security specifications. This helps address a growing need on the part of railway operators to better track who has accessed the network, and when, to enable them to identify the source of vulnerabilities and ideally who used the resulting back door. This long-term forensics capability is often also required by regulators.

7. Essential elements of in-depth security

There are some basic elements of effective cyber security for mission critical networks.

Automate security processes: First, today's manually intensive incident response approaches need to be automated. It's not uncommon for large critical network service providers to be bombarded with thousands of cyber-security alerts every day. Not all will be security breaches. Many will be false alerts and duplicate information. Yet, the sheer number of alerts can overwhelm a security team, leading to serious incidents not being investigated and followed up in time. They need better ways to automatically correlate, prioritize and deal with these alerts.

Furthermore, current approaches are inefficient, with up to 33 percent of incident response time is spent on manual processes, leading to delays. Combined with alert fatigue and time wasted on false calls, many security breaches can go undetected. Security automation that encompasses business processes, regulations and security policies will be essential to keep pace with the rapid rise in attacks.

End-to-end security is essential: End-to-end security is vital to protect all components of communications networks. Failing to address this will result in inadequate network protection and increase vulnerabilities to threats that are specific to one technology or another.

End-to-end security encompasses the operation of the entire network and its security processes, such as access management and audit compliance; network security, including signaling and core network security; and security management for IoT devices. Security management for devices must include three key components: secure identity management for each device, a secure communication channel between the management server and the devices, and a secure trusted software environment on each device.

An added complication is that fact that many such devices are unmanned and may not even have a conventional user interface. Also, many are meant to operate unattended for extended time periods, with no physical human interaction. The use of certificate management practices to ensure the identify and proper configuration of such devices before they are deployed in networks, is also essential.

[13] https://www.grahamcluley.com/train-control-centre-passwords-revealed/

[14] https://nakedsecurity.sophos.com/2012/08/24/security-tip-when-being-interviewed-on-tv-wipe-passwords-off-whiteboard/

Network segmentation and firewall: Network segmentation with IP/MPLS VPN based on rail applications or other policies provides traffic isolation and hampers lateral movement of hackers as they scout the network. With the frequency of DDoS attack on the rise, the network, together with network analytics platform, can also assume a critical role, acting as the first line of defense, filtering out network and transport layers attack traffic for the firewall to protect the network and infrastructure from more sophisticated application layer attacks.

Analytics for continuous improvement: Security analytics correlates data from across the network, devices and cloud layers to spot suspicious anomalies and provide insight into the nature of the threat, the associated business risk and recommended response. With machine learning, the effectiveness of security would increase continuously.

Encryption protects data: With encryption, even when a perpetrator taps into the communication channels, confidentiality, integrity and authenticity are still protected. As the network is deployed with different architecture and transport technology, it is vital to deploy multi-layer encryption that encrypts at the optical, IP, MPLS and transport layers. Encryption should also be applied to stored data, not just when it is being moved around.

High availability: Ensuring high availability and operational stability of the network and transport layers (for example on IP/MPLS, optical) is a key foundation for a secure network because it enables a rapid recovery from any attack, including physical shut down of communications equipment and infrastructure facilities.

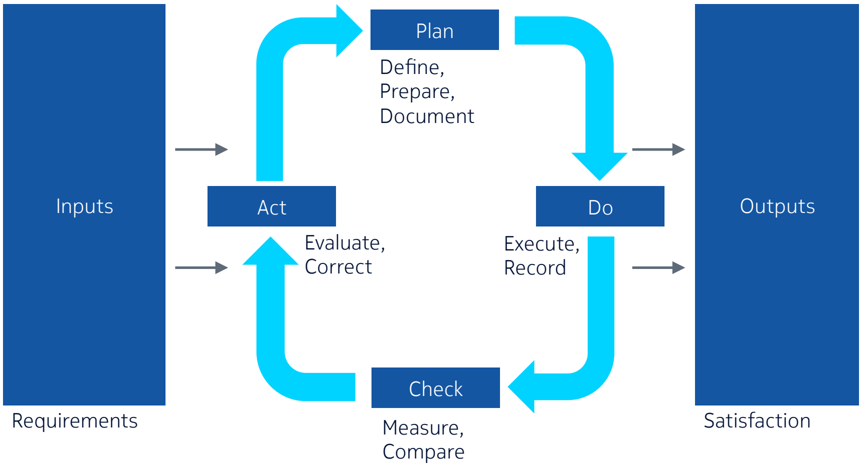
7.1 Implementing active security management

Various standards relating to security are available (see text panel "Standards for security"). There is also a wealth of best practices from mission-critical networks around the world, most of which advocate an active security management approach with automation and continuous improvement.

The traditional approach to security is largely based on manual processes without a centralized management system. This is still a reasonable approach for some organizations, but the increasing sophistication of attacks and growing regulatory complexity mean this will not be realistic in the medium term.

An expanded security management solution with analytics, automation and reporting would support workflow management and automation, analytics and reporting. This would enable security operations teams to automate and prioritize activities and report data to inform better business decision making.

Figure 4. ISO27001 is typical of the active security management approach to cyber security.



Standards for security

Examples of relevant security standards include:

ISO 2700x Information security management systems – ISO/IEC 27001 is the best-known standard in the family providing requirements for an Information Security Management System (ISMS).

ITU-T X.805 security architecture - a streamlined high-level threat model, enabling operators to assess network security and eliminate potential threats in complex environments. It can be applied across network operations, as well as in network management.

There are three layers to the architecture:

- The infrastructure layer, which comprises basic communications network building blocks such as routers, switches and transport equipment.
- The services layer, which comprises network services or circuits that deliver data generated by applications, such as supervisory control and data acquisition (SCADA), land mobile radio (LMR) or closed-circuit television (CCTV), end-to-end across the communications network.
- The application layer, which comprises the devices, simply known as endpoints, over which applications such as SCADA, video surveillance and IP telephony run. The endpoints could be a SCADA RTU, CCTV camera, SCADA server and Video Management System (VMS). An endpoint includes all associated hardware, software and firmware.

IEC 62443(-2-4) Security for industrial automation and control systems (IACS) – specifies requirements for digital security capabilities for IACS service providers during integration and maintenance of an automation solution.

EN 50126 The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – this is the railway sector specific application of IEC 61508.

EN 50128 Communications, signaling and processing systems – covers the software for railway control and protection systems.

EN50129 Communication, signaling and processing systems – specifies safety related electronic systems for signaling.

EN50159 Railway applications - Communication, signaling and processing systems – governs safety-related communication in transmission systems.

8. Nokia cyber security for railway communications networks

Nokia offers in-depth expertise in the development of cyber-security best practices.

The approach to mission critical cyber-security recommended by Nokia is based on a security framework that aligns an organization's different working groups and implements common best practices. The ITU-T X.805 security framework is used to help operators improve end-to-end network security and eliminate potential threats in complex, dynamic environments, and it can be applied across network operations and management.

Nokia end-to-end security solutions incorporate security products and services that address the specific challenges of rail operators. For example, the Nokia Netguard Security Management Center and Security Operations Analytics and Reporting platform enables security operations teams to automate and prioritize activities and report data to inform better business decision making.

Critical LTE network elements such as base stations, network controllers, mobile devices and application servers need to participate in their own defense. This self-defense capability is best developed during product design. The Design for Security (DFSec) approach used by Nokia deals with proactive security measures, including risk and threat analysis, secure OS configuration, access control, password policy, code review, penetration testing and other activities. Nokia also implements reactive security measures known as Security Vulnerability Monitoring (SVM) to ensure that OEM product vulnerabilities listed by computer emergency response teams (CERTs) are highlighted for further qualification and possible patches.

Nokia also applies best-in-class certificate management practices to ensure that IoT devices are properly identified and certified at the time they are deployed. Existing 4G LTE networks, and emerging 5G networks are designed with certificate management systems in place that are intended to deal with this challenge. Manufacturer-provided certificates with a unique, secure identifier can ensure that devices have not been modified or tampered with prior to deployment, and help ensure the identify of those devices once in operation. The large number of certificates and diversity of suppliers (certificate authorities) requires a significant effort to manage renewal and deployment tasks. Technologies which automate the enrollment and deployment of digital certificates can bring operational savings and prevent costly errors.

Nokia combines expertise in both LTE and IP to achieve mission-critical security that addresses the vulnerabilities specific to these technologies. Mission-critical network solutions (IP/MPLS, optical, LTE) not only deliver network reliability, performance and scalability, they are also an integral component of the security framework, defending against security threats and attacks. Nokia integrates security seamlessly with the existing operations support system (OSS), providing the relevant alarms, counters and monitoring capabilities without additional terminal applications or equipment. This enables the operator to focus on its mission-critical responsibilities without being distracted by the daily operation of a telecom business or by having to work with multiple security vendors to align on security roadmaps or incident resolution.

Nokia services provide the expert support rail operators need to secure their communications networks.

For example, the Nokia Security Risk Index (SRI) assessment framework and Managed Security Service (MSS) encompass all areas of security, including the assessment and continuous protection of multivendor networks.

With more than 30 years of experience in the rail industry, Nokia works with rail operators to develop proactive cyber-security for mission critical networks. Nokia security expertise is rooted in its strong presence in the public safety segment and as a trusted partner for public network operators around the world which impose the highest requirements for network security.

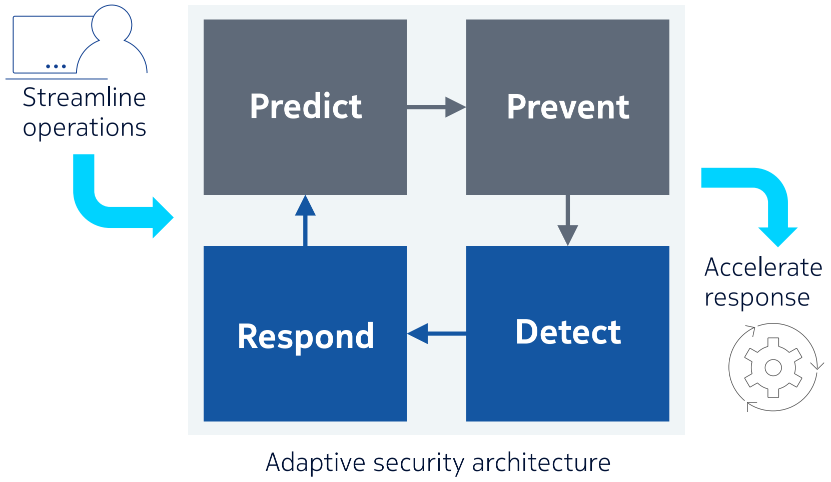


Figure 5. Security orchestration analytics and response transforms railway communications network security from manual and reactive to dynamic, Adaptive security architecture predictive and automated.

9. Conclusion

Hardly a day goes by without the media reporting a cyber-security incident or exposure of a risk somewhere in the world. Not only are attacks becoming ever-more sophisticated, but the potential damage that can result is growing, even physical damage to critical railway infrastructure such as signaling systems.

Railway infrastructure can ill afford any successful cyber-attacks. Not just financial loss is at stake; lives can be put in jeopardy.

At the same time, it is important for rail operators to evolve their communications towards new networking technologies, including LTE and IP/MPLS, to support new services and improve the efficiency of their operations. While such networks are future proof and scalable, they will introduce new vulnerabilities. With a robust network defense, these threats can be addressed.

Deploying the right level of security is a high priority. While all mission-critical networks are different, sound security typically requires a move from manual processes to automation, the application of data analytics and machine learning, end-to-end encryption and a full lifecycle evaluation of cyber-security risks.

Nokia offers an advanced and comprehensive approach built on its long experience and in-depth expertise of both security as well as mission critical networks design and operations. In line with best practices and published standards, the Nokia solution can ensure the highest levels of protection for railway communications.

Railways and the traveling public deserve nothing less.

For more information on our range of solutions and services for railways, please visit our railway page at https://www.nokia.com/networks/industries/railways/

10. Abbreviations

CCTV	Closed-Circuit Television
CERTS	Computer Emergency Response Teams
DDoS	Distributed Denial of Service
DeOS	Destruction of Service
DFSec	Design for Security
DWDM	Dense Wavelength Division Multiplexing
EPC	Evolved Packet Core
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Internet Protocol
IP/MPLS	IP Multiprotocol Label Switching
ISMS	Information Security Management System
KPI	Key Performance Indicator
LMR	Land Mobile Radio
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
OS	Operating Software
OSS	Operations Support System
SCADA	Supervisory Control and Data Acquisition
SS7	Signaling System No. 7
SVM	security vulnerability monitoring
VMS	Video Management System
VPN	Virtual Private Network

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 digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1907036767EN (July) CID201645