Verband der TÜV e.V.

TÜV®

Author
Richard Goebelt

Date
20 August 2019

Cybersecurity in a Digitally Connected Railway System

Digitalisation is fundamentally changing the mobility industry. The railway sector is facing increasing competition from other modes of transport. Above all, road transport is becoming more attractive compared to rail due to the rise of electric mobility, car sharing, and ridesharing as well as increasing levels of automation. Nevertheless, the railway sector is in an excellent position to benefit from the new digital potentials. Digitalisation improves the availability of rail vehicles and infrastructures, streamlines operations, and reduces labour and costs. It provides passengers with attractive and seamless mobility from A to B through shorter headways. It helps service providers make infrastructures more intelligent, improve travel comfort for passengers, guarantee availability, and sustainably increase added value over the entire life cycle, for example through data-based predictive maintenance.

On the other hand, the sector is exposed to new attacks in the area of security. As components become increasingly interconnected, more and more opportunities present themselves for hackers to infiltrate railway systems. Privacy protection is also becoming a challenge, as passengers expect their data and online services to be available at all times.

In this study, VdTÜV e.V. analyses which regulations need to be observed to ensure comprehensive security and which security measures are required. The growing threat of cyberattacks must be mitigated to allow manufacturers and system integrators in the railway sector to take full advantage of the opportunities offered by the new digital age.

Why cybersecurity management is vital in a digital railway infrastructure and connected railway vehicles

The systems and processes in a digital railway system must be continuously monitored in order to detect cyberattacks and react accordingly. Security in rail transport has traditionally been the purview of mechanics and engineering. Industrial systems used to be autonomous and were not connected to company networks or the Internet. Most railway systems were built before cybercrime posed a threat. This background fundamentally complicates the integration of state-of-the-art cybersecurity solutions into existing railway and metro networks.

Digitisation and networking so-called legacy systems such as relay interlocking poses particularly critical challenges with regard to cybersecurity, especially given the long product life cycles. These systems are often either completely unprotected or only weakly protected against cyberattacks, or they no longer meet the increasing demands on IT security. In an increasingly connected industrial world in the IIoT (Industrial Internet of Things), cybercriminals have a significantly higher number of potential targets at their disposal.

A digitally connected, non-self-contained railway system can no longer be regarded as functionally safe if the cybersecurity of the system has not been taken into account and competently assessed by an independent third party.

The digitisation of the railway system poses a number of fundamental challenges, including:

- High adaptation and implementation costs for new technologies
- IT security/data protection in general
- Ensuring the continuous availability of correct (uncorrupted) data (data integrity/availability)
- Connectivity and interoperability of different systems
- Conservatism in the industry, which can also be an advantage in terms of exercising caution

However, cybersecurity challenges do not only cover technical attacks and threats such as malware and viruses. IT security encompasses much more, including governance, risk management, security measures, and compliance monitoring. These issues also require attention in order to maintain an adequate level of maturity for digital safety in railway companies.

On the other hand, there are several advantages:

- Smooth intermodality (mobility platform in public transport, paperless ticket sales)
- Prediction of train delays
- Monitoring the condition of the infrastructure and the vehicle (predictive maintenance)
- Connecting vehicles, including across transport sectors

These potentials can be achieved, for example, by implementing the European Train Control System (ETCS) reference standard. Digital data transmission results in a more efficient interlocking architecture. However, the necessary intelligence required for this is no longer located in the hardware, but rather in the requisite software, which may also be distributed in a cloud. Hence, update capability is essential for smooth automated and connected railway operations.

Given the increasing prevalence of these new technologies, IT security is quickly becoming an indispensable component of railway company operations. Digital railway projects being implemented throughout Europe and the need for integration with other modes of transport also require the railway sector to open its borders to other actors in multimodal transport solutions. New regulations on cybersecurity, such as the Directive on the security of network and information systems (NIS Directive) and the General Data Protection Regulation (GDPR), require railway companies to maintain their standards to the greatest extent possible while meeting certain obligations resulting from relevant EU standards pursuant to Single Market legislation.

Cybersecurity is not only a high-tech and operational issue, but also affects the process level. Hence, the issue must fall under the purview of the top-level management of the respective companies.

Those responsible must ensure that appropriate measures are implemented and that the necessary resources are provided to effectively deploy a cybersecurity program within their companies.

Industry executives and security experts need to look for solutions that address the full spectrum of cyber vulnerabilities, efficiently detect threats, and block attacks before they compromise economic vitality and the safety of passengers. Cyber-solutions designed for railways must provide ongoing risk and threat assessments and update their security protocols.

What can be attacked, will be attacked – cyberattacks on the railway infrastructure

The threats posed by attacks on the railways are nothing new, as the following selection of incidents shows. In 2008, a Polish teenager hacked into the Lodz tram system, changed the track layout and subsequently caused the derailment of four trams, resulting in several injured passengers, but no fatalities[1]. According to Reuters News Agency, in 2016, North Korea tried to hack the email accounts of South Korean railway workers to attack the control system of the transport system[2]. In the same year, the British Independent reported that hackers had infiltrated the railway network in the United Kingdom up to four times in the year prior[3]. In 2017, the German rail network was plunged into chaos after being infected with the ransomware 'WannaCry': the information boards at German train stations displayed demands for ransom payments to restore access to the railway systems.

The main focus of these attacks is to impair the **reliability (safety)** and **availability** of the railway systems. An attacker could deliberately paralyse sections of the railway network for an indefinite period of time or attempt to undermine security systems. In addition to these 'real' obstructions, the trustworthiness and reputation of a company can also be negatively impacted in the event of a successful attack.

Given the connectedness of railway systems and the increasing professionalism of hackers, these types of complex attacks are likely to increase, possibly with more devastating consequences. In countries where millions of people depend on rail connections for their daily commute to and from work, a prolonged interruption of important rail systems following DDoS attacks[4] would wreak havoc on the local and national economy.

Governments and rail operators must therefore focus on implementing comprehensive and holistic cybersecurity solutions to guard against such threats. Achieving a constant time-independent level of security will no longer be possible: in light of ever-changing threats, new technologies and procedures, and the time it takes to address security vulnerabilities that present themselves, po-

[1] https://www.theregister.co.uk/2008/01/11/tram_hack/

[2] https://www.reuters.com/article/us-northkorea-southkorea-cyber/north-korea-Tried-to-hack-souths-railway-system-spy-agency-idUSKCN0WA0B6

[3] http://www.independent.co.uk/life-style/gadgets-and-tech/uk-rail-network-railways-hacked-four-time-hackers-trains-a7135026.html

[4] A DDoS attack is a special type of cybercrime. It stands for Distributed Denial of Service, i.e. an attempt to disrupt machine or network resources by flooding the system from multiple different sources.

tential attackers will always be capable of causing damage. Nevertheless, the goal must be to introduce technical and organisational measures to maintain information security at a level that is acceptable to all.

While the European Network and Information Security (NIS) Directive is an important step towards securing critical infrastructures, its provisions are too general and abstract with regard to the aforementioned risks for use cases specific to the railway industry.

Under the provisions of the Directive, Member States must ensure that essential service providers notify the authorities of cyber-incidents that have a "significant impact" on their services. However, the NIS policy unfortunately emphasises the exchange of information in the response phase, i.e. long after the threats have been discovered. Cyberattacks often appear insignificant at first, but can quickly snowball into critical events. Once a security vulnerability is discovered, the approval processes for railway technology are too slow to respond. The time it takes for a patch to be developed, tested for functionality and security, and approved by the respective authorities, the security vulnerability remains a target that can easily be exploited by attackers. Before a patch can be implemented, it must be certified not to cause any feedback effects on safety.

A more proactive approach would provide better protection against threats to key service providers. Regulatory adjustments and clarity in dealing with dynamics in security are imperative in this regard.

Security for safety – approaches to provide a modern safety assessment

In the past, railway infrastructure was predominantly viewed in isolation while operational or functional safety was the top priority.

The requirements for the functional safety of railway technology equipment are set out as follows in the national and European regulatory frameworks, e.g. in the EN 501XX CENELEC series:

- EN 50126 covers aspects of reliability, availability, maintainability, and safety (RAMS), both of the infrastructure as a whole and of individual subsystems.
- EN 50128 describes the process and technical requirements for the development of software for programmable electronic systems.
- EN 50129 applies to safety-relevant electronic signalling systems.
- EN 50159 applies to safety-relevant communication in transmission systems.

In view of the changing regulatory and normative safety requirements for conformity assessments, VdTÜV maintains that traditional assessment methods will no longer be sufficient in the future. In order to be considered safe and compliant, it is essential to keep vulnerabilities to a minimum by limiting the common resources, implementing coordinated protection profiles and optimally separating the systems from one another.

In contrast to functional safety, the assessment of cybersecurity represents a completely new challenge. The probability that a system is safe is an experience-based, statistical, or analytically determined quantity in the area of safety. This is not applicable to cybersecurity with its constantly changing threat landscape and its focus on ensuring confidentiality, integrity, and availability. The security of Internet-based systems and products with their own IP addresses and integrated software must be ensured throughout their entire product lifecycle and ecosystem. Due to updates and expanded functionalities that are no longer exclusively contained within the product, but rather in the 'backend' or product network, the definition of a product and the concept of product safety is beginning to shift. This is already reflected in the considerations on best practice approaches in cybersecurity and the definition of security by design systems currently taking place in the relevant railway committees CENELEC: WG26, ETSI:TC Cyber, and in the Shift2Rail consortium: TD 2.11.

Effectiveness studies for implemented security systems and cybersecurity risk assessments are becoming increasingly important in operations.

Cybersecurity risk assessments are designed to identify and analyse all relevant threats in order to derive appropriate measures to counter them. A distinction must be drawn here between the highly critical railway and train protection systems and the less critical areas of dispatching, passenger information, and ticketing. Malware analyses in the less critical areas show that several systems in the network display so-called IoC (Indicator of Compromise) alerts. These do not necessarily imply a critical attack in every case, but they do provide indications of threats.

In the interest of an interoperable and safe railway area, VdTÜV maintains that cybersecurity requirements must be codified in a cross-subsystem **Technical Specification for Interoperability (TSI)**. **Existing technical specifications and standards need to be harmonised to achieve uniform application.** The TSI could stipulate that cybersecurity was taken into account at every stage of development using a security-by-design approach. This would help improve the overall cybersecurity footprint of a system and increase its resilience to threats. At the same time, an international standard for cybersecurity in the railway system should be integrated into the international series of standards for "Industrial communication networks – Network and system security" (IEC 62443). The decision to develop a rail-specific adaptation and interpretation of IEC 62443 would mark an important first step. The future prTS 50701 will set a new benchmark in this regard.

In addition to establishing a cybersecurity architecture in the railway system, even more attention will have to be paid to the future implementation of robust, resilient architectures. The railway system and the respective operator must be better prepared for adverse conditions. The railway system must be able to maintain essential functions even under adverse conditions. Furthermore, the system must be equipped to fully recover its operational capability within a reasonable period of time. In this context, VdTÜV welcomes the published recommendations of the CYSIS working group "Resilient Architectures for Railway Signalling".

Importance of certifications to increase trust in cybersecurity

In order to improve protection against cyberattacks within the European Union, the EU Member States have adopted the 'Cybersecurity Act'. The European Union Agency for Network and Information Security (ENISA) is to be elevated to a Cybersecurity Agency. ENISA will receive a permanent mandate to assist EU Member States in effectively preventing and responding to cyberattacks. VdTÜV maintains that ENISA should support other European authorities such as ERA and actors in the railway sector in general in the development of cybersecurity strategies. It would also be desirable to form a network of experts for cybersecurity in the railway sector.

The draft Regulation also emphasises the creation of an EU framework for cybersecurity certification to increase trust in critical infrastructures such as energy and transport networks and Internet-based consumer products.

The proliferation of security-related incidents in recent years has shown that the 'duty-of-care' principle or the sole reliance on manufacturer responsibility alone is insufficient to guarantee an adequate level of security across the board.

VdTÜV therefore recommends that products, services, processes, and systems that involve a high level of risk should be subject to mandatory inspections to be carried out by independent third parties. A high risk exists if an attack on the integrity, confidentiality, or availability of the product or system could pose a threat to the health of users or third parties, the environment, or other essential legal interests (for example, unauthorised interference with privacy or property). Railway technology is fundamentally to be considered a high-risk sector, as it entails safety concerns that generally affect the core of the polity.

A certificate's statement regarding concretely defined IT security properties of an IoT product must be unambiguous, resilient, and transparent. Certification must always be conducted based on a depth of testing appropriate to the risk involved. The higher the risk of the IoT product, the deeper or more comprehensive the product testing must be. The certificate's statement must always merit the highest level of trust and be tied to the product-specific risk. Differences regarding the meaningfulness of a certificate must be derived from the declared testing criteria and procedures.

A conformity assessment by an independent third party is imperative to ensure the necessary trustworthiness and resilience of a certificate. If a manufacturer wishes to obtain a voluntary product, system, or service certification, it must be carried out by an accredited, independent third party that is not the manufacturer of the product or service, irrespective of the level of risk involved.

Summary

Digitalisation has arrived in the railway systems industry. Current reports on potentially vulnerable, modern railway systems make it clear that there is an urgent need for action to integrate information security into the security management process. The widespread use of commercial off-the-shelf software and easily accessible hacking tools increase the risk of cyberattacks.

The main focus of cyberattacks is on impairing the **reliability (safety)** and **availability** of railway systems. Manufacturers and system integrators in the railway industry must provide complete security and protection against cyberattacks for all their products and systems ('security for safety').

Cybersecurity is not only a high-tech and operational issue, but also affects the process level. Hence, the issue must fall under the purview of the top-level management of the respective companies. Those responsible must ensure that appropriate measures are implemented and that the necessary resources are provided to effectively deploy a cybersecurity program within their companies. A more proactive approach would provide better protection against threats to key service providers. Infrastructure operators should be aware that the operation of the railway system is at increased risk if hackers attempt to cause damage and disruptions. Operators must include cybersecurity risk as part of their broader risk management profile as soon as possible and ensure that all new systems and processes are secure and protected.

VdTÜV maintains that traditional assessment methods for railway technology will no longer be sufficient in the future in view of the changing regulatory and normative safety requirements for conformity assessments. Especially with regard to the aftersales market, it is crucial that appropriate processes and systems are applied in remote and inaccessible locations or infrastructures with limited capacity for system upgrades and updates.

Regulatory adjustments and clarity in dealing with dynamics in security are the order of the day. In the interest of an interoperable and safe railway area, VdTÜV maintains that cybersecurity requirements must be codified in a cross-subsystem **Technical Specification for Interoperability (TSI) to achieve uniform application.** Modern laws and requirements for cybersecurity and resilient architecture are required to protect railway customers and companies alike.