Cybersecurity and Safety on the Digital Railway

Point of View

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Introduction

Digitalization has arrived in railway systems as new interconnected systems and technologies are installed, benefitting operators, manufacturers and customers alike. Unfortunately alongside the benefits of these new services and systems there is an associated and growing risk of cybersecurity issues impacting the safe and efficient running of railway systems.

Cybersecurity is a new issue for many railway operators, system integrators and manufacturers, but today a connected railway solution can no longer be considered safe if it is not properly secured. The volume of new and emerging cybersecurity threats means that a system deemed safe at one moment may be rendered unsafe as new malware is released or a new attack vector established.

A digital railway system must now remain on a constant state of alert checking and monitoring its systems and processes from these threats.

But there is a challenge in addressing cybersecurity and safety in the rail industry. Legacy operational systems, many of which have been in place for decades, may receive an extension to their service life by providing them with a digital makeover that may not fully address cybersecurity related issues.

With the number of connected systems increasing there is a need for action to ensure the security and safety of the railway. Train operators need to maintain their reputation and the trust their passengers have in the railway system, as the success of rail transportation is arguably based on passengers' and customers' confidence in its safety, reliability and availability.

In addition many national governments have realized the importance of railways and classified them as part of their country's critical infrastructure that in turn has to be protected by implementing measures defined in national cybersecurity strategies.

Cyberthreats to the Railway

Railways face many of the same cyber related threats as other industries and sectors. As many railways modernise and adopt commercial "off the shelf" products, threats that are relevant to other sectors such as retail may now be just as applicable to the railway industry.

There are essentially two different types of IT system used on the railway;

- Business systems that provide the interface to customers and the information technology to support day to day commercial aspects of running a business including operator websites and ticket purchasing.

- Operational systems that directly impact the running of the railway including the infrastructure and rolling stock. Most if not all of these will be safety critical.

Some in the railway industry may question why the railway is a target for threat actors.

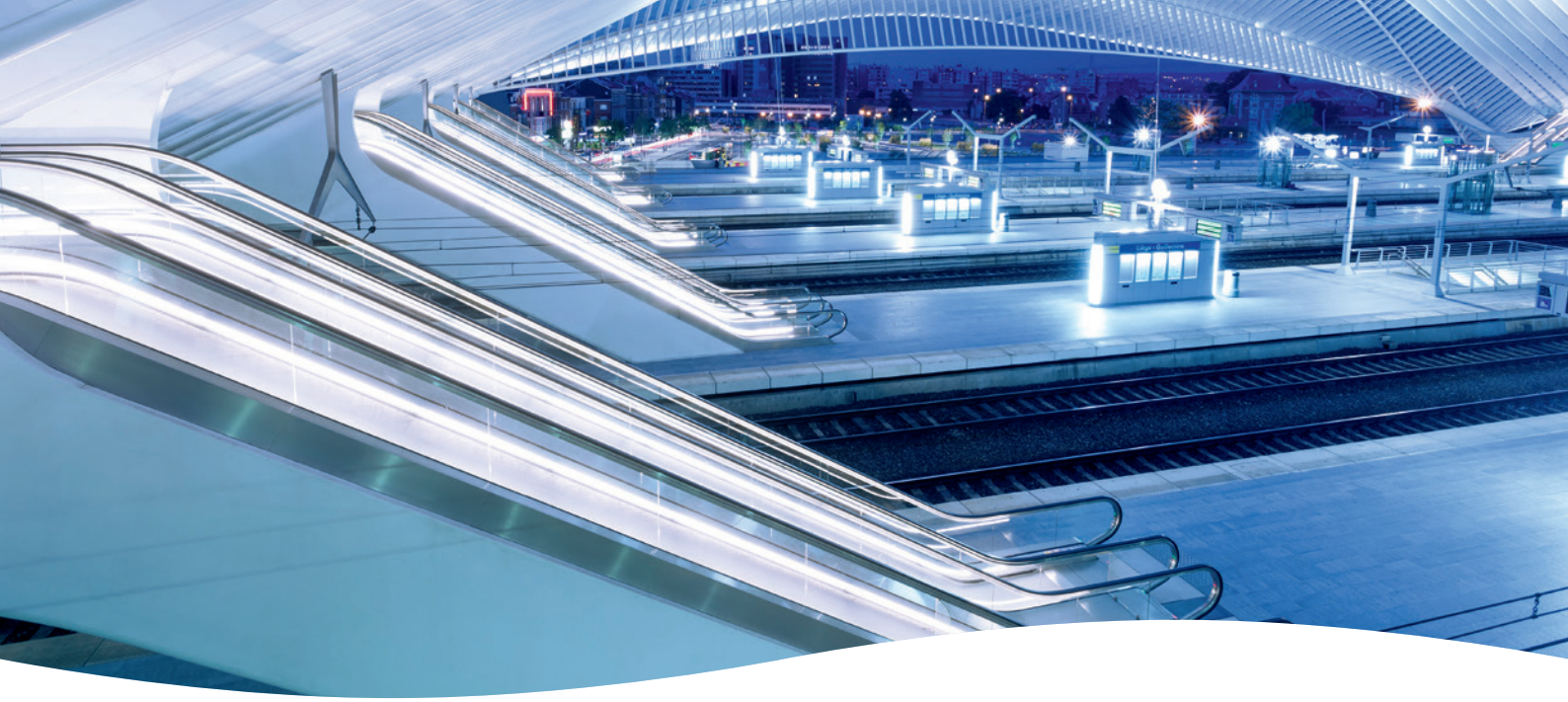
Alongside more conventional inside attacks originating from disgruntled employees or maybe those making a simple mistake, threat actors may see the railway as a "cool" target to attack. The impact of a cyberattack on a railway can range from a direct threat to passenger and staff safety, service disruption, reputational damage to operators, loss of intellectual property and even damage to processes or systems.

Passenger Information Systems

Most rail operators have enhanced or renewed their legacy passenger information systems at stations and in trains by adding a mobile system usually accessed using a smartphone app. Customers can now receive real-time information about their travel routes and purchase tickets.

Unfortunately by implementing such solutions additional cybersecurity risks are created.

Although railway passenger information systems are not safety critical, cyber incidents could have physical security consequences- for example passengers could be misdirected following a soccer match causing overcrowding or systems switched off resulting in chaotic scenes broadcast across media outlets.



Fixed Infrastructure Vulnerabilities

In addition to cybersecurity, physical security of the fixed railway infrastructure can be an immense challenge. In the UK alone metal theft from railway property costs over GBP £16 million per year (BSIA) and causes significant damage to the signaling and telecommunications infrastructure and knock on delays to passenger safety and services.

The often remote nature of such installations may also enable relatively easy access to equipment for cyberattacks. These could be in the form of plugging in a USB (thumb drive) containing malware into a remote lineside cabinet through to the interposing of control messages in short range wireless communications. As well as introducing safety issues a disrupted system could result in significant contractual costs due to delay cost attribution.

Computer Based Train Control (CBTC) Systems

Many rail systems worldwide are focussing on installing Computer Based Train Control (CBTC) or Positive Train Control (PTC) systems to increase capacity on the network by using a moving block signaling system to reduce train headway. For example European railways are starting to embrace the European Rail Traffic Management System (ERTMS) that makes use of common technologies including a Global System for Mobile Communications – Railway (GSM-R) for signaling, communications and train control.

Along with improved capacity, a CBTC system will normally have higher reliability, operational flexibility and be more energy efficient.

A cybersecurity attack on a train control system could ultimately impact the ability of the system to operate a train safely over a specific route within speed and stopping distances. This could theoretically result in a train stopping, colliding or derailing.

Possible attackable systems or components include the lineside beacons (balises), radio-based communications (including weakness of GSM-R security protocols), on-board units, control logic software of subsystems and centralised, regional signaling control rooms.

Safety and Cybersecurity in the Rail Industry

The railway environment is notoriously complex, bringing together often fast moving, highly energetic rail vehicles in close proximity to workers and passengers alike. Combined with high voltage power supplies, the carriage of hazardous materials and in many cases an overly stressed infrastructure safety has to remain a priority.

Newly commissioned rolling stock, operational systems and supporting infrastructure will inevitably make use of state of the art technologies many of which will be considered "smart" as they connect across the internet and World Wide Web. Similarly as older rail systems are retro-fitted with newer technologies many railways will operate in a hybrid technology world.

Regulations and Compliance Requirements

Safety standards have emerged such as EN 50126, EN 50128 and EN 50129 to support the creation of safe rail systems and associated hardware and software. But smart railway systems can no longer just rely on traditional risk methodologies to determine if they are safe, and indeed if they are not secure they are unlikely to be safe (Department for Transport (UK), 2016).

The full attention of the railway industry must now be given to ensure systems are both safe and secure.

This approach has been codified in IEC 61508, a general functional safety standard applicable to safety-related systems that incorporate electrical, electronic or programmable electronic devices (referred to as "E/E/PE"). The focus of this standard is on the failure of safety functions performed by a device, rather than hazards that might be generated by the device such as an electric shock. Key to achieving compliance to the standard is the need to "design in" functional safety from the start of product development.

It could be argued that the traditional railway failure mode is to a safe state, so that risks are addressed that way. Unfortunately the scale and scope of cyber related risk make such a guaranteed failure mode increasingly difficult to achieve, as not every conceivable cybersecurity attack mode could be planned for. In addition failure to a safe state will often mean, at best, a reduced operational through put (such as reduced speed of trains) through to system shut down as traction power is switched off. This could be seen as a denial of service attack in computer hacking vernacular.

As various railway safety and security standards evolve it is evident that safety and security will become even more entwined.

Where now and how can TÜV Rheinland help?

Rail industry manufacturers and system integrators should design in both safety and cybersecurity to all of their products and systems. Consideration needs to be given to after-market support of products and systems that may often be deployed in remote and inaccessible locations or infrastructures with limited opportunities for system upgrades and updates.

Rail operators should consider that the safe operation of their railway system is at increasing risk from threat actor's intent on causing damage and disruption. It is critical that operators now consider cybersecurity risk as part of their broader risk management profile and ensure that new systems and processes are both safe and secure.

Regulators are driving towards an inevitable increase in cybersecurity related legislation and requirements, so having processes and systems in place now to address this risk is crucial to protect rail customers and businesses alike.

In Summary

Rail operators must:

- Risk assess their IT and OT environments to benchmark their cybersecurity maturity.
- Regularly test IT and OT systems for vulnerabilities and ensure patches and fixes are applied as soon as possible.
- Ensure operational systems are implemented in such a way to minimise the likelihood of a cyberattack. This should include a mechanism to continually monitor such networks to detect possible intrusions.
- Ensure that new digital railway initiatives address cybersecurity issues from the start.
- Have an education program in place so that all employees and contractors are taught about cybersecurity risks.
- Implement an incident response and recovery plan to address any IT or OT cybersecurity incidents.

Rail industry integrators and manufacturers must:

- Ensure that security is designed into systems at the same time as safety issues are considered.
- Formally assess the security level of their relevant system so that potential operators can be assured that cybersecurity issues have been addressed.
- Provide an after-market mechanism for their system to be updated and maintained from a cybersecurity perspective.
- Proactively assist operators to install and configure their products in both a safe and secure way.

Rail industry manufacturers must:

- Ensure that security is designed into products at the same time as safety issues are considered.
- Formally assess the security level of their relevant products so that potential purchasers can be assured that cybersecurity issues have been addressed.
- Provide an after-market mechanism for their products to be updated and maintained from a cybersecurity perspective.
- Proactively assist integrators to install and configure their products in both a safe and secure way.

References

BSIA. (n.d.). Metal Theft- a guide to securing your business.
London: British Security Industry Association.

Department for Transport (UK). (2016). Rail Cyber Security Guidance to Industry.
London: Department for Transport.

European Cybersecurity Act. Proposal for a regulation- COM(2017)477/947932

Directive on security of network and information systems (NIS Directive)-
DIRECTIVE (EU) 2016/1148

TÜV Rheinland
ICT & Business Solutions
otsecurity@tuv.com

www.tuv.com/en/industrial-sec

TÜVRheinland®
Precisely Right.