Cybersecurity in railway signalling systems

Prepared on behalf of the IRSE International Technical Committee by Norbert Howe

The purpose of the IRSE's International Technical Committee (ITC) is to provide thought leadership and disseminate learning on technical topics relevant to train control and communication systems. This provides value not only to IRSE members but also to the wider rail industry. The committee's particular strength lies in its international membership, enabling engineering principles and practices from a diverse range of countries to be brought to bear upon the subjects that are debated.

In this report Norbert Howe describes the challenges and potential approaches associated with the cybersecurity of railway signalling and control systems.

Introduction

Computer based signalling systems have been introduced in the late eighties and successfully deployed and evolved in the years since, being assessed and approved for safety based on an evolving set of norms and regulations, especially EN 50129 (IEC 62425).

Implementing and providing safe travel on rail is one of the core objectives of all partners in the business, from suppliers, engineering companies, operators, rail infrastructure providers and network operators to certification and assessment bodies.

Systems are evolving along with customer requirements; harmonisation and standardisation efforts are undertaken and implemented in order to increase the capacity and performance of the system, and to enable international travel and operation without additional efforts on the borders of national railway systems.

Considering these aspects, one could think that the evolution of signalling systems was continuing within well-defined and stable framework conditions.

However, at least in recent years, railway signalling systems cannot be considered as self-contained any longer and new kinds of threats have to be considered and taken care of, related to the fact that the railway signalling systems are more and more wide-spread, highly integrated and communication-based. Based on these core aspects, additional vulnerabilities have to be considered related to aspects as increasing integration with non-signalling subsystems and aging technology in legacy systems which have been put into operation long before the current threat level has evolved. All these so-called "*cyber threats*" are requiring new measures and efforts in order to ensure the integrity and safety of the railway system – and they cannot be considered to be taken by one of the business partners alone.

In the scope of this article, security and safety are referred to based on the following definitions:

- Security: Comprises all measures that are taken to protect a place or an item against espionage or sabotage, crime, attack or escape, or to ensure that only people with permission enter or leave it [9, 10].
- Safety: Comprises all measures that are taken to ensure that travel and traffic on rail is being performed without accidents causing injuries or fatalities.

Recent evolution

Over the last few years, there have been significant evolutions which have increased the relevance of cybersecurity considerations and measures.

The operation of signalling systems until recently has been considered to be performed using closed networks – and this assumption has been taken as the basis for the safety assessments performed before approving the systems for use. In recent years, the infrastructure-related signalling systems are getting more and more centralised and integrated – the assumption or pre-condition that any unauthorised access can be excluded and thus the system is operated within closed networks is no longer sustainable or realistic.

At the same time, railway signalling systems have become more and more software and IT-based, providing functionality which is not solely hosted on dedicated computers or hardware but on servers which are similar to IT systems.

In parallel, over the last years, the threats for IT systems have significantly grown, from sporadic amateur-driven access attempts towards well-organised cyber attacks. Examples include:

- Intrusion into the Lodz tram point control system (2009) [1].
- De-activating the ticketing system in San Francisco´s public transport system (MUNI, 2016) [1].
- The so-called "*Wannacry*" attack in May 2017, which infected more than 200,000 computers world-wide, including passenger information screens at railway stations [2] (Figure 1).

Figure 1 – The recent 'Wannacry' outbreak affected passenger information screens. *Photo Shutterstock/Egorev Artem.*

This being the case, active threats for the signalling system have to be taken into account:

- Safety is operationally being ensured by the implementation of the approaches stipulated by the CENELEC norms, basically ensuring safe operation by proving the probability of incidents is below the defined thresholds as shown by the risk analysis for all reasonable degraded situations and failures of parts of the system.
- Security has to ensure safe operation of the system in the presence of active threats and measures taken against the safe functioning of the system.

Moreover, it has to be taken into account, that even non-safety-relevant security breaches could cause major performance decreases or even outages, in a world where the high performance of rail networks is crucial.

Threats are becoming bigger

In early times, attacks on computer systems have been led by so called 'script kiddies' trying to show that they were able to enter systems which were thought to be well secured.

Over the last years, a well-organised scene has evolved with groups of specialists, stable or for a period of time, who are threatening and maliciously attacking computer networks.

A whole crime scene has evolved in this area, aiming at acquiring data, access codes etc. in order to steal money, intellectual property or to harm or destroy the business and operation of the target under attack. One example is selling stolen data or by encrypting the system, and as such make it unable to perform its function, then demanding a ransom to release it; so called 'ransomware'.

All in all, the number of attacks on computer systems has dramatically grown over recent years, which has led to a remarkable statement, condensing the status: "*There are only two types of companies: Those who have been hacked and those who don´t know it.*" (James Comey, 2014).

Railway signalling systems are not exempt from these attacks, which has very recently shown in the course of the so-called "*Wannacry*" attack [2],. Attacks like this may not directly violate safety as they are not able to infect the core of the vital subsystems but they can – and "*Wannacry*" already has – infected parts of the disposition and passenger information systems. In consequence, the operation of the railway network, its performance and capacity would directly deteriorate.

As the signalling system is getting more and more integrated and is extending its geographical and communication reach, it gets increasingly interesting to hackers. This has already been the case over the last few years [6].

Systems have evolved and exposure has grown

During recent years, the framework conditions regarding travel, including rail, have been evolving. Traveller numbers have increased and prognosis show that they will continue to increase in the near future. The requirements of customers towards online information and a seamless transport and journey experience have grown significantly. Amongst others, these aspects have led to an evolution of the signalling and rail transportation system , whose key subjects are:

- The request of customers for online information on travel connections and their current state leads to higher integration of systems. This includes the non-vital, formerly separate subsystems as schedules, actual trip status data, etc.
- The relevance of data has been increasing significantly, data being scattered over the constituents of the system.
- Systems have become more and more IT-based, applications running partly on dedicated, but partly on standard IT infrastructure, such as servers.
- Operation and maintenance of the systems being provided in a distributed manner over the subsystems and components of the system, according to roles and needs.

In parallel, the rail transportation system has been fragmented to an increasing degree related to legislation and market opening initiatives, fostering the separation of Railway Undertakings and Infrastructure Managers. Thus, in addressing a system relevant subject such as cybersecurity, an increasing number of stakeholders will have to be included.

Awareness and approach

A normative framework has been established

Starting from a Standard of Good Practice (SoGP, Information Security Forum, London) and the Consortium for Research on Information Security and Policy (CRISP, Stanford University) in the 1990's, guidance and norms have been developed, covering the subject from different perspectives. During the last 10 years a core set of norms has evolved which is being updated regularly, of which the most important are:

- NIST800-53, part of the US government's National Institute for Standards and Technology (NIST) Cybersecurity Framework [7], defining security and privacy controls for Federal Information Systems and Organisations.
- ISO/IEC 27000-series, an information management security system (ISMS) standard.
- ISA/IEC 62443, defining rules and procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

The Legal Framework has been set up

In parallel, a legal framework has grown and been elaborated in order to define the minimum standards to be applied. The European Union and its governments consider the risk for the functioning of the societies and their main supportive systems as critical. They have identified the need to secure these critical infrastructures on a European and not on a country-by-country level.

Thus, the European Union has taken legal action and put into place the network and information security (NIS) directive [5,8] which aims at securing the key critical infrastructures. This directive has been adopted by the European Parliament on 6 July, 2016 and will be enshrined in national law by 2018.

The railway network is considered as one of the most important critical infrastructures to be secured against cyber attacks and consequent harm, comparable to power plants and electrical power distribution systems, drinking water, road and public transport and shortly behind national health systems and the military.

The organisations implementing and operating critical infrastructures are asked to set up measures and plans in order to ensure their defence against cyber attacks.

There is only one promising approach – the system view

Ensuring security against cyber attacks is not a one-time task to be fulfilled during design of the system, it is a continuing task to be performed throughout the operational life time of the signalling system.

The evolution of systems and their integration to ever higher degrees in combination with rising communication needs increases the vulnerability of rail transport systems to cyber threats as compared to earlier times.

In rail transport systems the two disciplines of safety and security have to be distinguished. Safety, which has evolved over many years and is highly regulated, implemented and well understood, is concerned with the protection of life and property

through regulation, management and technology. Security is covering the confidentiality, privacy, availability and integrity of the system.

Security adds to safety but should not be mixed with it – it is like two sides of the same coin, but they have to be looked at and covered separately. Why?

- Update cycles for the signalling system are much longer than those needed for the security coverage.
- Even though design and constructive precautionary measures will be taken, security updates may be needed frequently, comparable to common IT.

It will not be possible to keep safety case and coverage of security completely independent, but the relation between both will have to be carefully constructed. An unmanaged interference of security into the safety case has to be avoided under all circumstances in order not to invalidate the safety case by updating the security measures in the system and thus creating an effort which would be difficult to master. Safety case validation is normally a time-consuming and diligent process whereas the response to cyber threats must be rapid.

For security considerations, in the system which the railway signalling system constitutes, the approach to cybersecurity has to be a system-oriented one, as well. Considering only single products or system constituents will not be sufficient. Products and subsystems will have to be hardened for security nonetheless as a prerequisite.

Cybersecurity has to encompass technical elements as well as organisational regulations, for both, customer and supplier. Thus, the approach to security has to be holistic; it will have to cover at least three dimensions, technological, social and procedural [4], also see Figure 2.

Moreover, it has to be considered that the railway system is not owned by a single, integrated organisation or entity, but is also distributed over different stakeholders – from Railway Infrastructure provider to the different Railway Undertakings, in addition there are multiple interfaces between parts of the railway network not least at country borders.

In this way, cybersecurity cannot simply be "*delivered*", it has to be engineered and designed into the system and implemented in collaboration between suppliers, customers and governmental bodies, building on their combined knowledge of railway technology, operations, risk assessment, its coverage and safety as well as IT security.

The implementation of this joint approach is not limited to a specific phase of the life cycle of the railway signalling system, for example the design and implementation phase. It has also to be seen and implemented in a holistic way over the whole life time of the signalling system, from its conception up to its decommissioning. This deep and continuous collaboration across the different functions active in the railway sector, Railway Infrastructure provider, Railway Undertaking, suppliers, governmental bodies as well as security experts is key to success.

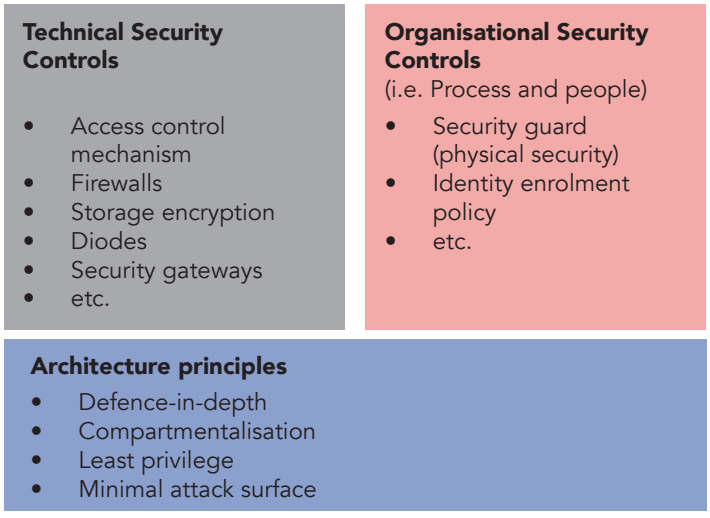

Figure 2 – Multi-dimensional approach to security.

All partners have to contribute

The conviction that railway networks are being safely operated based on the safe design of the systems developed, installed and operated based on rules and regulations which have been proven over decades, sometimes seems to lead to a low awareness of the risk which these distributed control systems are facing.

This picture and awareness are currently hopefully changing with stakeholders increasing their involvement and focus on the subject [3]. Amongst others, several large railways are currently bringing together their expertise and are driving forward the standardisation of signalling system interfaces and related cybersecurity capabilities, having realised that single approaches will not lead to a successful solution. This EULYNX initiative is, in this respect, defining a standard security architecture and in line with it, specifications for cryptography, firewalls and networks as well as for methods like download and diagnosis. These definitions should be in line with the governing security standards and enable the railways to identify and explicitly address, which aspects need to be covered on top by the different actors.

Thus, the task to ensure security of the system cannot be successfully performed by the operator itself, it is an exercise to which different roles and parties have to contribute in order to be successful – customers, suppliers and assessment bodies.

Eight ways to protect the railway signalling

As explained earlier, there are different norms providing basis for the coverage of cybersecurity, ranging from more engineering and industrial control focus to less descriptive but more holistic approaches. IEC 62443 is tending more to the first group whereas the NIST is intending to address the subject entirely. The NIST Cybersecurity Framework provides a comprehensive view on the way to detect, deter and cope with cyber-attacks on critical infrastructures.

The approach has to be comprehensive and NIST provides a framework which helps to address the complex subject accordingly. It structures the subject into the phases shown in Figure 3 overleaf. Additionally, it provides Security Control Baselines:

- Grouped according to subjects.
- Classified into pre-defined types (low impact – high impact).
- Containing sets of measures/priorities.

Finally, there is the Security Control Catalogue, proposing approaches and details.

The NIST cybersecurity Framework can be taken and understood as a comprehensive guideline. In itself, it is a huge and complex work – which gives an indication that the subject of cybersecurity itself will not be closed and covered easily.

Based on this process oriented approach, the following eight ways to establish and enhance cybersecurity seem relevant:

1. **Establish cybersecurity design principles**

Develop a mind-set for security within the organisation and apply design rules on several levels of the system architecture.

2. **Create a stronger perimeter**

Apply strong measures such as Security Gateways and Web Application Firewalls and VPN on the external interfaces.

3. **Deploy system security and detection/recovery controls**

A Security Information and Event Management Solution (SIEM) and centralised antivirus platforms should be used in order to immediately alert those responsible for security.

Functions	Functions roles	Categories
IDENTIFY	Develop the organisational understanding to manage cybersecurity risk to systems, assets, data and capabilities.	Asset management, Business environment, Governance, Risk assessment, Risk management strategy
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access control, Awareness and training, Data security, Information protection processes and procedures
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and events, Security continuous monitoring, Detection processes
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response planning, Communications, Analysis Mitigation, Improvements
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery planning, Improvements, Communications

Figure 3 – NIST cybersecurity framework phases.

4. Meet cybersecurity standards

Follow industry best practices by implementing according to strong standards.

5. Embed cybersecurity in the project life cycle

Signalling system projects have to incorporate and apply security measures during all phases – from bid to testing and putting into operation.

6. Establish and perform risk assessments and penetration testing

Map the threats and vulnerabilities for each asset of the system and establish a clear view on the related cybersecurity risk. Ensure the implementation of the relevant measures and perform penetration tests in order to verify their effectiveness.

7. Maintain good operational conditions

Apply and regularly check the application of clear rules and procedures in order to keep up the level of security management throughout the system lifetime, including updates and system changes.

8. Mandate safety protection

Implement measures to ensure message integrity and safety control in order to safeguard the system against unauthorised messages and malicious software.

Conclusion

Within a railway command and control system the approach to cybersecurity has to be a system-oriented activity, as part of the overall 'system engineering' approach and covering the whole life-span of the system. Considering only single products will not be sufficient. Products and subsystems will have to be hardened for security nonetheless.

The architecture has to incorporate measures and capabilities to implement security, thus the rail control system needs to be implemented according to a security architecture which is aligned with the safety architecture and overall architecture: "*cybersecure by design*" is one indispensable prerequisite to achieve security of the whole system. In addition, process and social aspects need to be covered in order to ensure secure operation, maintenance and use of the system throughout its lifecycle.

Threats are increasing in number – and have reached significantly high numbers of attacks per day already. Threats evolve quickly – so implementing and operating secure systems will require swift action and adaptability. Suppliers and customers need to address the subject jointly and quickly in order to take the right measures in a well aligned way.

Following a comprehensive scheme as explained above, based on the NIST approach and supporting signalling system network standardisation initiatives can help the different actors to align their views and approaches to cybersecurity in order to collaborate effectively.

It has to be realised and accepted that the effort to secure our railway signalling systems and railway networks against cyber-attacks has just begun. It will constitute a significant effort during the coming years – but it is unavoidable in order to match up to the evolution of threats.

References

[1] Bull, John, 12 May 2017, "*You hacked: cybersecurity and the railways*", in: Reconnections – London Transport and beyond. ***irse.info/gawo9***

[2] Ward, Marc, 16 May 2017, "*WannaCry and the malware hall of fame*", in: BBC News Technology. ***irse.info/jf7e9***

[3] Poisson, Pascal and Poré, Jacques, "*Signalling Control Systems – Innovations and Future Developments*", in IRSE NEWS 209, March 2015, pages 2-8

[4] Bastow, Michael, "*Cybersecurity of Railway Signalling and Control System*", IRSE ASPECT 2015.

[5] Kessell, Clive, "*Cybersecurity – The Network and Information Security Directive (NIS) and the legal position in the UK*", in IRSE NEWS 226, October 2016, pages 23-25

[6] Voudouris, Christos and Gibbons, Peter, "*Securing the Digital Railway*", in IRSE NEWS 227, October 2016, pages 9-13

[7] "*Security and Privacy Controls for Federal Information Systems and Organisations.*" NIST Special Publication 800-53, Revision 4. January 2015.

[8] European Commission Digital Single Market - Directive on security of network and information systems (NIS), July 2016.

[9] Collins Dictionary, ***www.collinsdictionary.com***

[10] Merriam-Webster Dictionary, ***www.merriam-webster.com***