Challenges and Approaches in Securing Safety-Relevant Railway Signalling

Christian Schlehuber*, Markus Heinrich†, Tsvetoslava Vateva-Gurova‡,
Stefan Katzenbeisser†, and Neeraj Suri‡
*DB Netz AG
christian.schlehuber@deutschebahn.com
†Security Engineering Group, TU Darmstadt
{heinrich, katzenbeisser}@seceng.informatik.tu-darmstadt.de
‡DEEDS, TU Darmstadt
vateva@deeds.informatik.tu-darmstadt.de
suri@cs.tu-darmstadt.de

***Abstract*—The railway domain is a complex critical infrastructure (CI) linking communication and control elements, and susceptible to multiple security threats similar to those encountered by industrial control systems. However, protecting modern railway signalling systems is a challenging task given the rigorous human safety standards that must be adhered to while augmenting the systems with security mechanisms. As railway CIs are subject to strong regulation and also cannot be adequately protected by physical security given that they are distributed over large areas, the strong interplay of security and safety requirements results in both unique problems and solutions. In this paper, we describe the current state of railway signalling, the obstacles to consider when protecting signalling using state of the art information security, and also outline contemporary approaches to address such obstacles. Overall, we propose a shell concept as an approach to decouple safety and security.**

***Index Terms*—Critical Infrastructure Protection, Railway Safety, Information Security, Railway Signalling Networks, Industrial Control System**

1. Introduction

Control and safety systems play a central role in the safe operation of rail networks. In the early days, circa 1900, the safety of trains was ensured by mechanical interlockings. Since then, the interlocking systems have evolved to result in complex electronic interlocking schemas. As a part of this evolution in functionality and distribution, the general architecture and behaviour of the interlockings have also changed. While in the beginning only a minimum of interaction with external systems was required, the modern electronic interlockings or operations control centers (OCC) are invariably connected to a wide variety of internal and external systems. Also, while most communication transpires on dedicated networks, the current trend, driven by functionality and costs, is to increasingly utilize public communication channels as well.

Each new interlocking design aims at improvements to the protective safety functions in response to previous incidents. This continuous improvement process has resulted in railway transportation being one of the safest public infrastructures. However, in recent years new challenges for the control and safety systems have risen from a change in societal and usage threats. Additionally, the tighter coupling of systems and diminishing error-tolerance thresholds (for economic reasons) imply higher damage consequences.

In the earlier years, the greatest threats for the railway transportation were either technical or human errors, i.e., operational errors caused by the actors of the system. Only in rare cases were the errors caused intentionally by actors external to the system.

Unfortunately, modern railway systems are increasingly attacked by external adversaries [1]–[3]. These types of deliberate attacks on control and safety systems have primarily been considered at only an incipient level. Due to the increasing attacks by external actors and the also the increasing potential for damage, these are no longer incidental issues and require be addressed comprehensively to also handle the new technological developments.

This development is also empowered by the currently ongoing digitalization and standardization of control-command and signalling systems, which is driven by the aim of railway operators for a better performance and a lower price of interlocking components. Consequently, commercial off-the-shelf (COTS) components are increasingly being used to develop safety-relevant components. In addition, standard commercial network equipment, along with standard protocols are utilized, and the systems are connected through backbone networks to enable the control of several track regions by a single control center.

Our work focuses on the track-side train control systems, i.e. the signalling system as described in Section 3 that includes the interlocking and the field elements. Signalling systems have their counterpart in rolling stock to realize concepts like Automatic Train Protection (ATP), such as

PZB[1] and LZB[2] in Germany and ETCS[3]. However, rolling stock is out of scope for this work.

Figure 1 highlights the range of challenges that arise for electronic interlockings and also outlines attack surfaces for the various sub-components of an electronic interlocking system (ESTW[4]). The graphic shows the basic building blocks of a NeuPro-ESTW using standard components, standard protocols and a method for loading new software to interlocking components remotely. Each of these methods, aimed at performance enhancements, also increases the attack surface of the system. For example the standard IP networks enable an attacker to perform attacks on the interlocking system, which were originally developed for different environments (e.g. general business IT) and with different legislative perspectives to address system security.

As public transport is essential in our everyday life, it is unambiguously categorized as a Critical Infrastructure (CI). The national and European legislation is currently establishing new laws that require operators to ensure the availability of their service even under attack scenarios. The German IT-Sicherheitsgesetz (IT Security Law) has been enacted in July 2015 and is an example for a national law on CIs. On European level, the Network and Information Security (NIS) directive [4] entered into force in August 2016 and will also have an influence on modern interlocking architecture, as can be seen in Figure 1.

Given the changing technological and legal situation, the railway operators are required to extend their safety systems with security technologies to ensure that an attacker is not able to have any negative influence on the safety of the system.

However, simply introducing security is not as easy as it may appear. Security and safety are related, but are also very different domains with different terminologies, assumptions, processes and objectives. Safety deals with hazards inside the system due to malfunctions or hardware failures, while security addresses attackers that actively want to manipulate a system. Also, security often relies on reactive approaches, such as fast patching when a new exploit is found. In contrast, safety-related systems cannot be directly patched without a full consideration of operational and regulatory conformance implications on the overall system. If a change is introduced that could have an effect on the safety-relevant parts of the system, then a new admission by the National Safety Authority is required. This entails a comprehensive cause-effect analysis that typically takes several months. Due to such constraints, the introduction of security elements into the domain of railway signalling has to be done carefully. In this context, our work presents approaches for introducing security solutions without affecting the safety-relevant parts of the system.

This paper is organized as follows. Section 2 lists projects and references relevant to the railway domain. Section 3 explains the basic architecture of signalling networks along with the relevant safety requirements. Section 4 presents our approach to enhance safety with security. Section 5 presents our summary conclusions.

2. Related Work

Currently, only some limited initiatives exist for addressing security issues in the railway domain that arise as a result of the digitalization in this field. One of these is the German working group CYSIS[5] in which industrial and academic partners collaborate to investigate security problems in the railway infrastructure. The Control and Communications Security (CCS) Working Group published recommended practices for the American Public Transportation Association [5]. This report identifies the need for cybersecurity in rail transit environments, and stresses integrity and availability as the most important security properties of the digitalized signalling systems. According to the recommendations of the CCS Working Group, the assets to be protected should be identified and characterized based on their safety criticality levels. These recommendations raise awareness regarding the security in the railway systems. The partners of the SECRET (SECurity of Railways against Electromagnetic aTtacks)[6] project realized the importance of signalling systems security. This work aimed at preventing the exploitation of the vulnerabilities due to electromagnetic disturbances in the railway systems. SECRET proposes an approach for preventing the European Rail Traffic Management System (ERTMS) from electromagnetic attacks, by assessing the risk, identifying vulnerable areas and making railway communication resilient to these attacks. Another project focusing on security and safety in the digitalized signalling systems is ARGUS [6]. The aim of the project is to issue best practices for ensuring the efficient use of networks without having a negative impact on safety or performance. The main outcome of the ARGUS project is a handbook to ease the task of integrating the collected information into an international standard. A prerequisite for designing a good security strategy in railway signalling according to the project is to take into account the network security, the deployment security and the signalling security. Risk analysis and assessment models that consider tolerable and intolerable risks are also proposed. The Future of Surface Transport Research Rail (Foster Rail) project funded by the European Commission (EC) also identifies the importance of security in the railway domain [7]. The outcome of the project should serve as a basis for future strategic rail research. It consists of part-roadmaps based on the same template and thus, sharing the same structure and description to facilitate interoperability and integration.

Despite the existence of varied security standards, virtually none of them can easily be mapped to the railway domain to address its specific security requirements and

1. German: Punktförmige Zugbeeinflussung
2. German: Linienzugbeeinflussung
3. European Train Control System
4. German: Elektronisches Stellwerk

5. https://www.cysec.tu-darmstadt.de/de/news-events/events/vergangene-veranstaltungen/cysis-gruendungssymposium
6. http://www.secret-project.eu/

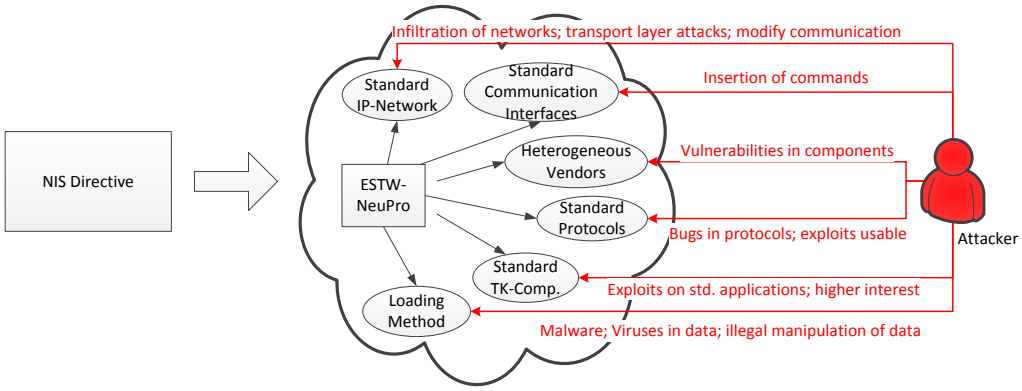

Figure 1. Challenges due to technological and legal changes

issues. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published the 27000-series comprising information security standards [8]. They provide recommendations for best practices and are very broad in scope, making them applicable to a large number of areas. Still, the 27000-series is not created particularly for the railway domain and thus does not consider the characteristics of the signalling systems. Another relevant standard is IEC 62443 on network and system security with focus on industrial-process measurement and control. IEC 62443 is also not focused explicitly on signalling systems and cannot be directly mapped to the railway domain [9], but it has been used as a basis for the creation of a important German prestandard, namely DIN VDE V 0831-104 [10]. It provides guidelines for security analysis approach. DIN VDE V 0831-104 defines system security requirements in signalling systems and security levels depending on the motivation of the attacker and its capabilities, as proposed in IEC 62443. None of the above mentioned standards considers augmenting safety and security in the railway domain explicitly.

Smith et al. investigate "Security as a Safety Issue in Rail Communications" and show the fundamentals of safety and security engineering [11]. The paper shows that the engineering concepts are similar to the ones we imply. However, it does not discuss the strict safety regulations that need to be considered for European railway communications.

3. Signalling Networks

This section describes the architecture of a typical signalling network and the requisite safety requirements that apply for building and operating it. It is important to examine the basic architecture and the characteristics of railway signalling in order to understand the decisions that need to be made when introducing information security solutions onto it. We also discuss the currently utilized communication networks and the necessary safety requirements.

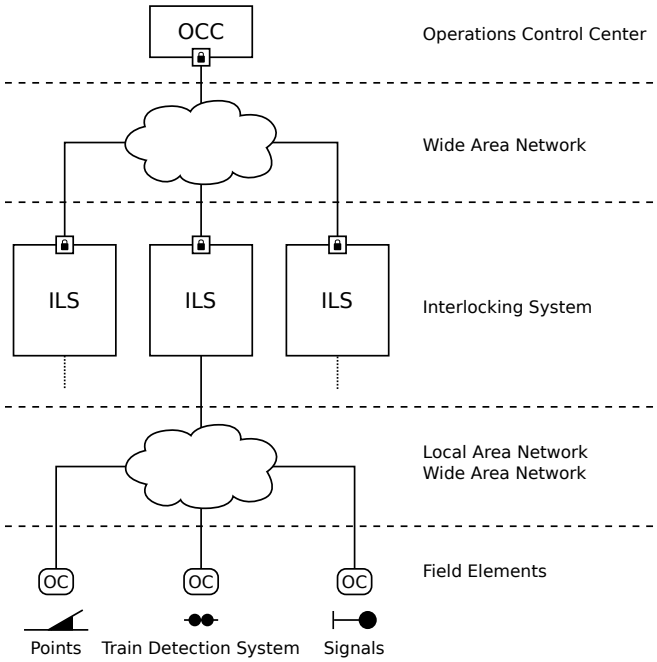

Figure 2. Architecture of a typical signalling network

3.1. Network architecture

The architecture of modern signalling networks comprises of three main levels linked via a communication network, as schematically depicted in Figure 2. The progression from the lowest level comprises of the field elements, followed by the interlocking system (ILS) and the top level Operations Control Center (OCC).

The basic building blocks of safe train movement are summarized under the term "field elements". The signals, points, and train detection systems (TDS) constitute the sensors and actuators of the railway system. Signals are the main means of communication between the traffic supervisor and the train driver, while the points determine the

route the train will take. The TDS reports to the interlocking system whether a section is currently occupied by a train. On this level the safety functions are executed, e.g. by separating two trains from each other with a signal showing the aspect *stop*. This is one of the methods to avoid collision of trains. The field elements are driven by object controllers (OC) that translate between digital commands from the ILS and control signals (e.g. for the point machine).

The dependencies between field elements that ensure the correct and safe operation of trains are modelled in the ILS. Its logic excludes operations on the field elements that are hazardous in the current state of the interlocking. The ILS holds a model to distinguish safe states of the infrastructure that can also be used to determine legitimate messages in the network, as presented in Section 3.2. Modern interlocking systems rely on computers to realise the logic needed to control the field elements and are therefore called electronic interlocking. Each ILS is responsible for a well-defined area of tracks with their field elements, resulting in the need for vertical communication in the depicted architecture. An interlocking area can cover a single station, multiple stations, or parts of a station, depending on the operational size (i.e. the number of field elements to be operated).

Mainly for business management reasons, the supervision of an ILS can be further centralized in the OCC. This centralization provides a better view of the train movement through the overall network and shortens the communication channels between the supervisors. There is no safety-relevant need for this centralization, as the field elements and interlocking systems provide safe train movement on their own. A traffic supervisor is located in the OCC or the interlocking building depending on organisational considerations. He operates the ILS and is responsible for the correct routing of trains.

3.2. Utilized communication networks

The communication between the entities increasingly utilizes standard protocols like Ethernet or IP, but also specialized protocols like RaSTA[7] [12] that provide better guarantees to availability and timeliness. This is required to fulfil the standard on safety-related communication EN 50159 [13].

In the area of an interlocking system, the interlocking computer and the field elements are connected through a distinct local area network (LAN). There is no need for the field elements to be accessible from outside the interlocking area, as this would increase the attack surface. However, it is prohibitively expensive to build a dedicated network to handle the communication between an ILS and the OCC given the large physical distance and the spatial distribution of the interlockings. Therefore, commercially available wide area networks (WAN) are used, which then necessitate the needed means of protection against intruders. One countermeasure is a railway specific virtual private network (VPN) that is built between the partners of a communication channel through the WAN, indicated by the small lock icons in Figure 2. The supervision of moving trains is passed from interlocking to interlocking. Thus, the systems need to commuicate the train data to neighbouring systems, which means that they need to communicate horizontally with each other. This is also done over the same WAN that connects the interlockings to the OCC. Recent developments utilize WANs between interlocking systems and field elements as well, instead of a distinct LAN, which is an advantage in larger interlocking areas.

7. Rail-Safe Transport Application

3.3. Safety requirements

Each building block of a signalling system, including the field elements and the interlocking, is designed to be fail-safe. For a signal this means that in case of a failure (e.g. the connection to the ILS breaks down) it will take a safe state, showing the signal aspect *stop*. Beyond this, there is no awareness of the track layout or the safety logic at the level of field elements, which means that they do not have any notion about the safe movement of trains. This responsibility is solely taken on by the interlocking. The fail-safe principle further requires that any failure is revealed in a timely manner – a requirement that applies to any component used in signalling that fulfils a safety function.

There are several established standards on the European level that regulate developing and manufacturing safety-relevant railway applications including signalling systems. EN 50126 [14] defines the management of reliability, availability, maintainability, and safety (RAMS). These four aspects allow the assessment of systems that are put in place in the railway domain. The standard enables an optimal combination of RAMS for a stipulated cost for a system, and also supports the cooperation of railway operators and manufacturers. The availability of a system is considered to be the composition of a high reliability and good maintainability. For every function an interlocking system fulfils, there is a fall-back level that can overtake operation in case of a failure in the primary level. Because of the fall-back levels, reliability and safety are closely coupled, as the fall-back normally provides less safety but prevents the system from becoming unavailable. The standard forces operators and manufactures to consider and implement the RAMS requirements in order to build a system with high quality. The international standard IEC 62278 [15] corresponds to and is derived from EN 50126.

EN 50128 [16] defines methods to develop software for a safety-critical environment. This includes applications, operating systems, and firmware, as well as tools that support their development. On international level, EN 50128 is adopted by IEC 62279 [17]. According to these standards, building dependable software requires having the process, the documentation, and experts in place. First, a model of the desired function is defined against which the software will be verified. Subsequently, the model is tested in a real world scenario to validate that it fulfils its stipulated purpose. The steps are embedded in a standard V-Model

Table 1. OPEN AND CLOSED TRANSMISSION SYSTEMS ACCORDING TO EN 50159

Property	Closed (Cat 1)	Open (Cat 2 + 3)
Number of users	limited	unlimited
Unauthorized access	excluded	possible
Physical properties	known	possibly unknown

that covers the definition and implementation of the system on the left side and the tests and integration on the right. The software developed for safety-critical signalling networks subsequently needs to be certified by EN 50128.

EN 50129 [18] describes the lifecycle of safety-related electronic systems for signalling and is an important standard regarding safety.

EN 50159 [13] describes safety-related communication in closed and open transmission systems and is therefore relevant for the aforementioned networks between field elements, interlocking systems and OCCs. The utilized transmission system itself does not need to fulfil high safety standards, because they are provided by the safety-critical communication process on top of the network. Closed transmission systems – also called Category 1 networks – feature a limited amount of users, exclude unauthorized access and have defined physical properties. Therefore, it is only required to protect the communication from bit errors, message delays, and connection losses. Open transmission systems have contrary features, as summarized in Table 1. In particular, unauthorized access can no longer be excluded, such that the standard requires the safety-critical communication system to protect authenticity, integrity, timeliness, and sequence of the messages. The standard distinguishes open transmission systems between Category 2 and Category 3 networks. However, we investigate open transmission systems in general and mention the distinction for completeness only. These requirements apply to the presented communication networks in order to guarantee safe train operation. On international level, EN 50159 is used as a basis for the creation of IEC 62280 [19].

Running a network in the signalling domain is very different from running a general communication network. Any human error during the development, implementation or operation of a safety-critical system can likely pose a threat to human life. Thus, railway operators must present a safety case, which needs to be accepted by the National Safety Authority in order to be allowed to run the examined system. The safety case categorically ensures that it has taken care of avoiding or mitigating the risk of the safety-critical systems according to the European Standards EN 50126, EN 50128, EN 50129, and EN 50159. Any changes in the hardware, software, or other parts of the system need to be reflected in the safety case, probably requiring its reconsideration.

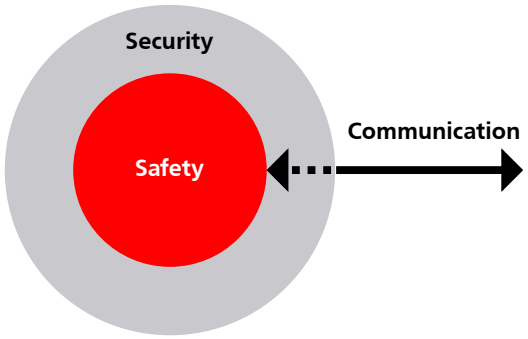

Figure 3. Security for Safety shell

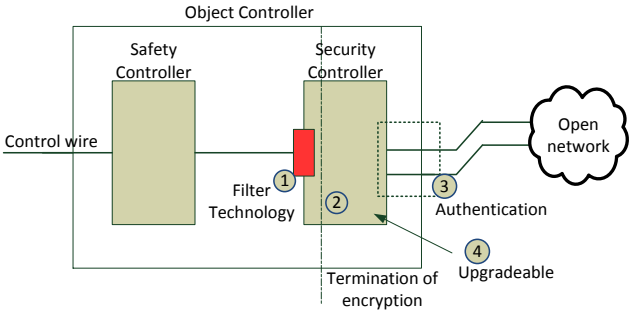

Figure 4. Separation of Safety and Security parts

4. Security for Safety

"Security for Safety" is one of the prominent current topics in railway engineering. Several groups consisting of vendors, operators and research are discussing solutions, which allow to bring these domains together without having negative effects.

We propose a "shell" concept to approach this issue. An abstract view of the shell is illustrated in Figure 3. In the shell concept, we surround the safety-relevant system with another system to ensures security. Every communication channel has to pass the security shell before it can reach the safety-relevant system. Apart from adding the security component, the safety-relevant system also has to be hardened according to its functionality. The proposed separation brings several advantages:

- In case we have to apply a patch to the security system due to a change in the threat landscape, we can do this without having to go through the admission process for the safety system, because we only have to ensure, that the interface to the safety system is the same.
- We can separate the operation and maintenance of the components easily.
- If an attacker performs a DoS over the network, only the security system is taken down, the safety-relevant component can fall into a safe state until the security component becomes available again.

The concept is illustrated in Figure 4, which shows the advantages of this design. In this example the object controller, which provides the safe operation of the signalling system's field elements, is enhanced by a security component. This component can be used to introduce a large variety of security features to the OC. One of the security features is cryptography. In our scenario we are flexible enough to adapt to changes in technology, such that cryptographic algorithms can be exchanged easily. Besides the possibility to encrypt the communication, the security component could also implement a filter mechanism, which later on can be updated on a regular basis with respect to upcoming attack vectors. With this, a quick response to detected attacks is possible. Subsequently, the vulnerability in the safety-related software itself can be fixed in its regular patch cycles to ensure an in-depth security concept.

Currently, a system design is being developed for the railway track fields according to the former mentioned principle. The current OCs are not capable to provide enough security functionality and various issues related to patching of safety-components in case of a vulnerability exist. Because of this, a security box is placed between the OC and the WAN. The security box encrypts the communication to ensure integrity and confidentiality, even though confidentiality is not important in our case. The encryption is based on a public key infrastructure. If an attacker attacks the OC, he has to break the encryption as replay attacks are detected by the safety protocol RaSTA. Additionally, the security box makes use of white list filtering and only the commands for the specific interlocking component are allowed to pass through the filter. If an attacker finds a way to pass all these lines of defence and is able to compromise the safety component, an analysis of the log would show the steps taken and an additional filter could be applied within short time to the security box to mitigate the attack.

As illustrated by the separation of the components according to their domains (security and safety), each component could behave according to the requirements of its domain. The admitted (and also static) safety component is only changed during regular patch intervals, while the security component can be adapted as the corporate security process requires. The effort reduces to demonstrating that the interface to the safety component has not been changed in a negative way and the needed performance indicators are fulfilled. With this we can bring together the different velocities of updating safety and security systems.

Another benefit of the mentioned design is that the security/safety incidents can be clearly identified. In current systems it is hard to determine, whether an outage was security- or safety-related. With our proposed design, distinguishing across security and safety incidents could be done according to the location of the outage. If the security component fails, it will most likely be a security incident, otherwise safety is more likely.

To enable such a separation, the interlocking system and the employed protocols have to be clearly specified with key performance indicators (KPI) and also with precise specification of the interfaces between them. These are needed to be chosen such that the RAMS requirements of the system can be based on them. One of the KPIs could be availability, for instance. The safety component requires a certain availability of the security system to fulfil its own requirements. If the security component fulfils the set KPIs, the safety component is also able to fulfil its requirements. If a change to the security component is done, only the defined KPIs have to be proven to ensure the safety case is still valid. The KPIs have to be included in the admission of the safety component. This also applies to the used communication channels which means that there have to be Quality-of-Service mechanisms and traffic has to be categorized as well as priorities have to be assigned.

It needs to be ensured that the security component has no negative effect on the safety component.

5. Conclusion

We have reviewed the domain of railway signalling which is dominated by safety requirements that challenge the integration of today's information technology, and especially as the safety and security lifecycles differ. The discussed network structure represents the generic German railway architecture though it is comparable to the infrastructure of railway operators in other European countries where the same standards apply. On this background, we have proposed an approach to prepare the networks for defending against attacks that can compromise information security and consequently the system safety.

The efforts to enhance international security standards for industrial control with railway specific requirements have not yet yielded a CENELEC[8] standard. This leaves the industry, operators, and research in a state where it is not clear as to which level of security is necessary to obtain the admission of the National Safety Authorities. However, the German prestandard DIN VDE V 0831-104 [10] points out which direction the application of security will take in the railway domain. The approach is to apply the internationally recognised but in parts not yet published IEC 62443 [9] in order to not re-invent the wheel.

Fulfilling the standards will be necessary to receive the admission to operate railway infrastructure. Our approach to encapsulate the safety-critical function into a layer of security is compliant to them, as it would not be applicable otherwise. Note that this approach does not aim to provide only perimeter-level security, as the proposed scheme is applicable across the architecture layers to establish a defence in depth concept.

Our proposed shell concept separates safety- and security-related systems in a way that enables clear distinction between their responsibilities and simplifies the safety case. The shell concept can employ various mechanisms that have been developed by information security. This includes digital signatures, encryption, and anomaly detection. The latter can exploit the special conditions of a signalling network. These are the rather static architecture of the network,

8. European Committee for Electrotechnical Standardization

that is unlikely to change on short notice, and the exact model of which messages are expected in the network which exists in the ILS. It has to be investigated to which extent the model can be reused by shifting the logic towards the field elements in order to check the plausibility of commands and eventually detecting anomalies.

This example shows how the shell concept will be used in future work to apply security mechanisms to the architecture of signalling networks. Signalling networks utilize interfaces between infrastructure and vehicles that can be looked at from a security perspective. This includes national train protection systems, called Class B systems in ERTMS, as well as the communication systems and on-board unit of ETCS itself, but is beyond the scope of this paper.

While little academic literature exists for railway security, several industrial projects are ongoing in this area. However, to the best of our knowledge, none of the efforts is dealing with the necessity of security coupled with the constraints imposed by safety requirements. This motivates the need for further research in the composite saftey-security arena.

Acknowledgements

Research supported in part by EC H2020 CIPSEC GA 700378.

References

[1] J. Riley, "Terrorism and Rail Security," RAND Corporation Testimony, Tech. Rep. CT-224, March 2004. [Online]. Available: http://www.rand.org/pubs/testimonies/CT224.html

[2] J. D. Ballard, "A Preliminary Study of Sabotage and Terrorism as Transportation Risk Factors associated with the proposed Yucca Mountain high-level Nuclear Facility," School of Criminal Justice - Grand Valley State University, Tech. Rep. NWPO-TN-018096, Sept 1997.

[3] Supreme Audit Institution of India, "Performance Audit on Security Management in Indian Railways," Tech. Rep. 14 of 2011-12 (Railways), Aug 2011. [Online]. Available: http://cag.gov.in/content/report-no-14-2011-performance-audit-security-management-indian-railways-union-government

[4] European Parliament and European Council, "Directive (EU) 2016/1148 (NIS)," 2016.

[5] American Public Transportation Association, "Securing Control and Communications Systems in Rail Transit Environments," Tech. Rep. APTA-SS-CCS-RP-002-13, June 2013. [Online]. Available: http://www.apta.com/resources/standards/documents/apta-ss-ccs-rp-002-13.pdf

[6] International Union of Railways (UIC), "ARGUS Project," 2015. [Online]. Available: http://www.uic.org/com/uic-e-news/392/article/argus-kick-off-meeting-paris-19?page=thickbox_enews

[7] D. Schut, V. Kinderis, U. Meuser, C. Hilgers, and R. Müller, "Deliverable D4.1 Delivery of the final template for Technology and Innovation Roadmaps. Foster Rail." Grant Agreement 605734, 2013. [Online]. Available: http://www.errac.org/wp-content/uploads/2013/07/FR_WP4_UIC_D4-1_-Final_For_Upload_2.pdf

[8] ISO, "ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary," Tech. Rep. BS ISO/IEC 27000:2014, May 2009.

[9] International Electrotechnical Commission, "IEC 62443 Industrial communication networks – Network and system security," IEC 62443, Nov 2010.

[10] DKE, "Elektrische Bahn-Signalanlagen – Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage der IEC 62443 (DIN VDE V 0831-104)," 2014.

[11] J. Smith, S. Russell, and M. Looi, "Security as a safety issue in rail communications," in *Proceedings of the 8th Australian workshop on Safety critical systems and software-Volume 33*. Australian Computer Society, Inc., 2003, pp. 79–88.

[12] DKE, "Electric signalling systems for railways – Part 200: Safe transmission protocol according to DIN EN 50159 (DIN VDE V 0831-200)," 2015.

[13] Comité Européen de Normalisation Électrotechnique; english: European Committee for Electrotechnical Standardization (CENELEC), "EN 50159: Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems," 2010.

[14] ——, "EN 50126: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," 1999.

[15] International Electrotechnical Commission, "IEC 62278 Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)," IEC 62278, 2002.

[16] Comité Européen de Normalisation Électrotechnique; english: European Committee for Electrotechnical Standardization (CENELEC), "EN 50128: Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems," 2012.

[17] International Electrotechnical Commission, "IEC 62279 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems," IEC 62279, 2015.

[18] Comité Européen de Normalisation Électrotechnique; english: European Committee for Electrotechnical Standardization (CENELEC), "EN 50129: Railway applications – Communiations, signalling and processing systems – Safety related electronic systems for signalling," 2003.

[19] International Electrotechnical Commission, "IEC 62280 Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems," IEC 62280, 2014.