Implications of Cyber Security to Safety Approval in Railway

Eivind H. Okstad

SINTEF Digital, Norway. E-mail: eivind.h.okstad@sintef.no

Robert Bains

SINTEF Digital, Norway. E-mail: robert.bains@sintef.no

Thor Myklebust

SINTEF Digital, Norway. E-mail: thor.myklebust@sintef.no

Martin G. Jaatun

SINTEF Digital, Norway. E-mail: martin.g.jaatun@sintef.no

The railway domain has a justifiable preoccupation with safety, but less of a focus on cyber security. This could result in the risk of cyber security flaws in current railway systems being unacceptably high. However, in recent years the railway industry has realized the importance of cyber security, and the possible effects cyber security could have on safety functions, necessitating these aspects to also be considered as part of the safety approval. This trend can be seen from the fact that later updates of the railway standards from CENELEC to a larger degree include cyber security. This is also a consequence of the increasing digitalisation trend in the railway sector, as elsewhere in society (e.g., the ERTMS national implementation project in Norway). This paper presents findings from a brief literature study on how railway systems are vulnerable to cyber security threats and discusses how cyber security issues are covered by current railway legislation. Challenges related to the handling of cyber security threats as part of the railway approval processes is then elaborated. The fact that cyber security threats change faster than the pure safety threats must be taken into account. The problem is viewed from an independent safety assessor's point of view. Some major findings of the study are elaborated, and conclusions on how to deal with cyber security as part of the railway approval process are outlined with pros and cons.

Keywords: Railway, Cyber security, Safety, Approval, Legislation, Standardization

1. Introduction

It could be argued that there is insufficient focus on cyber security in the railway domain, where more emphasis is placed on safety and efficiency. There is reason to believe that this situation has resulted in the existence of cyber security flaws in current railway systems as mentioned by e.g., Gabriel, et al. (2018). This situation implies a meeting of two different professional cultures (Line, et al. 2006). Safety culture in railways is invoked through a rigid approval process. ICT security, on the other hand, is often characterized by the need for frequent security patching as e.g., the telecommunications industry uses frequent software updates (patching) for security reasons. One challenge may be related to the fact that those who work within the railway approval process traditionally are safety people having less knowledge of the cyber security people, and how they tend to work. In this paper, cyber security is applied as a common term for any cyber security aspects, like IT-security and ICT-security, often used in literature.

Threat landscapes of threats against railway systems, or System Under Consideration (SuC) according to the IEC EN 62443 standards, are discussed by Rekik, et al. (2018a). However, in recent years the railway industry has realized the importance of cyber security aspects in addition to safety as part of the safety approval of railway systems. This can be seen from the fact that railway safety standards, such as CENELEC EN 50129 (2018), and EN 50159 (2010), to a larger degree include requirements related to cyber security, or ICT-security issues. In addition to these two standards, EN 50126-1/2 (2017) and EN 50128 (2011) are normative safety standards addressing the RAMS process and software process requirements, respectively. These two standards, however, do not address cyber security in a particular manner.

Because of the digitalisation trend in railway, it is important to reflect on cyber security in the context of safety approval of railway systems since cyber security threats could have implications on functional safety. Cyber security threats typically change at a faster pace than pure safety threats, and new threats occur after the system is put into service. Due to the comprehensive approval processes in railway, the handling of cyber security threats become even more complicated compared to other industries. Integrating the safety- and security processes may have pros and cons, but this article addresses some challenges that need to be addressed in the railway legislation.

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper

A second goal is to elaborate on how relevant challenges could be handled efficiently as part of the railway approval process.

1.1. *Study approach*

Starting out with a literature study, we discuss cyber security in the context of safety regulation and elaborate on possible impacts on the railway approval process based on our experience as safety assessors. The following topics are addressed in the paper:

- Section 2 presents findings from the brief literature study on cyber vulnerabilities related to safety in railway, and the handling of cyber security.
- Section 3 discusses the safety approval process and how cyber security is covered by current regulation.
- Section 4 addresses the coming regulation to incorporate cyber security explicitly.
- Finally, in Section 5 we elaborate on challenges related to the handling of cyber security as part of the future railway approval process.

The literature study includes a search for earlier work that touches upon topics of cyber security and safety in railway systems. In addition, an overview of ongoing work in EU regarding cyber security within the railway domain is provided. Here, the recent ENISA study (Liveri, et al., 2020) focuses on the level of maturity of the European railway sector regarding implementation of security measures as enforced by the NIS Directive (EU Parliament, 2016). On the standardization front, CENELEC plans to issue the technical specification TS 50701 in mid-2021, which aims to introduce requirements as well as recommendations to cyber security within the railway sector.

2. Railway cyber security and safety - a literature study

Several studies exist that investigate cyber vulnerabilities and threats to railway systems and related infrastructures. This paper emphasises cyber security aspects of main relevance to safety in railway, but also other aspects of importance to understand how to best handle and maintain cyber security within the domain. In this section, Train control and monitoring systems (TCMS) is addressed as an example of cyber-threat target, whereas Section 3 focuses on signalling systems as the authors' experience is mostly with such sub-systems.

2.1. *Cyber security in railway safety assessments*

Train control and monitoring systems (TCMS) are continuously improved using networked control and automation systems and connected technologies (Rekik, et al., 2018a). Cyber-physical security concerns are thus relevant for these systems. As such, vulnerabilities and characteristics of the railway threat landscape need to be analysed. The work of Rekik, et al. (2018b) addresses threats to TCMS, and tries to identify convenient security countermeasures, i.e., defining the adequate protection levels for each of the TCMS assets. A somewhat broader threat landscape has been addressed. As an example, the cyber-physical security risk assessment of one functionality of TCMS, namely the external door control, is presented in Rekik, et al. (2018b). This study refers to the IEC EN 62443 framework of standards that provides guidance to improve cyber security and help reducing the security risks of systems under control (both hardware and software). The security risk assessment methodology proposed by IEC EN 62443-3-2 (2020) is composed of 13 steps and applies the included SuC delimitation.

Another study of Kertis & Prochazkova (2018) looked at control systems in railway applications, seeking to derive evidence/learning from railway accidents related to possible deficiencies in design of the control systems. The paper presents four examples (Case studies) of railway accidents that demonstrate consequences of control system designs, which contributed to the accidents. These accidents were from the Czech Republic, Spain, Germany and the USA. Relevance to the present study is the risk potential from cyber threats against the control systems.

There is probably much to learn from other domains or industrial applications dealing with cyber security. Industrial control systems and automotive are domains in which a cyber-physical approach to cyber security is developing fast (Pizzi, 2020). Knowledge and results from here are applicable to railway systems as well. References are also made to the main IT security standards and to those standards supporting the industrial sector like EN ISO/IEC 27001 (2013), EN ISO/IEC 27005 (2018), and the IEC 62443-series.

As an overall risk analysis of the system, Pizzi (2020) suggests a fault tree approach leading to an attack-fault-tree method for analysis of hazards and threats, as part of the co-engineering of safety and cyber security. Some more analytical approaches to security and cyber security aspects within the process safety domain are proposed by Cormier & Ng (2020) and Śliwiński (2018). The first one discusses the significance of incorporating cyber security vulnerability analysis in terms of protecting a process control network. In addition to traditional process hazard analysis (PHA), a layer of protection analysis (LOPA) is adapted to implement adequate safeguards against cyber threats. These methods can integrate cyber threats into the risk analysis in a unifying way that strengthens resilience to both cyber- and traditional risk. The work of Śliwiński (2018) highlights some important issues of the functional safety analysis, in particular the safety integrity level (SIL) verification of safety functions. Such a verification is implemented within distributed control and protection systems regarding cyber security aspects. A method for SIL-verification, based on the so-called differential factor is presented. As an addition to SIL, a safety and security impact reference model (SSIRM) is presented by Pawlik (2019), which, is based on identification of functions supported by electronic, digital, and programmable solutions. The model was used to prepare a set of questions related to essential functionalities.

Another approach to security risk management in the railway industry is presented by Tillema (2017). The "Thameslink Programme" here highlighted a method for managing cyber security related to safety critical railway

systems involving a cyber security risk register that is verified, validated, and maintained by all stakeholders in the scope of the system. A perceived threat assessment is conducted that lists potential attackers and scores their motivation and capabilities. Potential threats may here include elements such as foreign intelligence services, serious organised crime, terrorism, as well as insiders and authorised users.

2.2. *Typical threats and vulnerabilities*

As mentioned above, potential threats against TCMS are widespread. A threat taxonomy is presented in Rekik, et al. (2018b) that covers mainly cyber security threats directed specifically towards ICT assets, thus affecting SuC operations. This taxonomy was based on the studies of the European Union Agency for Network and Information Security (ENISA, 2015, and ENISA, 2016a.b.), published in Dimitra et al. (2020) with recent clarifications. Threats are here classified into the following:

- Physical threats. This type of threats may cause intentional offensive actions aiming to achieve maximum distraction, disruption, destruction, exposure, alteration, theft or unauthorized accessing of assets such as infrastructure, hardware, or ICT connections.
- Accidental acts or faults (e.g., disasters and outages, failure, and malfunctions). Possible incidents are results of unintentional insider actions including human errors. Unintentional mistakes can be made by authorized employees, users, developers, and testers during data entry, operations, or system or application development. Such errors can affect system integrity and stability.
- Malicious acts. This type of threat comprises cyber-attacks and intentional nefarious activities or abuse targeting railway system assets through the digital assets.

Another study of Beecroft (2019) was a review of evidence that considered future security of travel by public transport, by addressing three main questions: 1) What are the current security challenges for public transport networks? 2) What are the emerging future security challenges? and 3) What technologies will have the biggest impact on security of public transport in the near future? Six transport security themes were addressed, namely a) Threat detection and prevention, b) Crisis management, c) Cyber security privacy and ICT, d) Staff security training, e) Cargo security, f) Passenger security.

A perspective of cyber security in railway was found in the context of eMaintenance in Thaduri, et al. (2019). There is an increasing trend in data-driven decision-making algorithms for effective design, construction, operation, and maintenance of infrastructure, mainly due to the digitization trend. Possible breaches and leak of data to the wrong hands might result in risks, loss of trust, as well as other serious consequences. eMaintenance focuses on the potential challenges and management of data security in the railway infrastructure. Systems being exposed to cyber security in railway are typically the electronic interlocking systems, level crossing protection systems, automatic block signalling systems, track-vehicle transmission systems and additional systems aimed at communication and failure detection.

2.3. *To secure cyber-physical systems by design*

Different approaches exist to achieve or obtain secure cyber-physical systems by design. For building railway infrastructures, Levshun et al. (2020) propose a solution in sense of a methodology based on trade-off between resources and security. The key idea here is to provide the most rational solutions that improve security of cyber-physical systems. Solutions are called alternatives and are built according to functional requirements and non-functional limitations imposed on the system. The methodology combines elements of design methods, development-, and verification techniques within a single approach. Each cycle of the methodology consists of a verification process and seven stages that are associated with the used cyber–physical system model. Verification occurs after each stage as many times as necessary to build the verified model or prototype of the cyber physical system. As being an integral part of the proposed methodology, the verification process provides the formal check of the system creation (possibility) in accordance with the requirements and limitations, as well as checking that the designed system is secured against attackers of certain types/levels. Proper assessment and treatment of safety-related cyber threats is important safety documentation. Thus, the connection to the safety approval processes and regulation in the next sections is obvious.

3. The safety approval processes

Safety approval of railway signalling systems are today based on among other the CENELEC standards EN 50126-1/2 (2017), EN 50128 (2011), EN 50129 (2018) and EN 50159 (2010). The main emphasis of the approval of e.g., railway signalling systems, are on safety, however, cyber security (or IT-security as mentioned in the CENELEC standards for railway) are also addressed. Whereas the focus in EN 50126-1/2 (2017) and EN 50128 (2011) are on safety and quality, EN 50129 (2018) and EN 50159 (2010) also include requirements related to cyber security in the context of OT (operational technology), as seen in Fig 1.

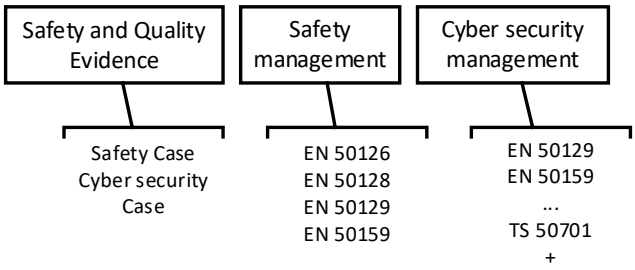

Fig. 1. Safety and Quality evidence, and the valid regulations

EN 50129 (2018), which requires that the quality- and safety evidence is collected in a top-level document called Safety Case, states that the safety management

process aims at minimizing the residual risk of safety-related systematic faults and security threats (including IT-security threats) so far as safety is concerned. It is further required that IT-security threats are managed during risk assessment and hazard control if an impact of IT-security on functional safety is reasonably foreseeable and cannot be excluded by simple arguments (e.g., a system having no connection to untrusted networks).

Railway signalling systems communicate through transmission systems. Directly relevant to the Safety Case, as required by EN 50129 (2018), is the documentation of what kind of transmission system is used and what kind of communication measures are implemented in the signalling system in order to ensure a secure communication. EN 50159 (2010) includes requirements to signalling system's safety-related communication in transmission systems. The standard defines three categories ranging from closed type of transmission system to a fully open transmission system (untrusted networks) of transmission systems. It further states which threats could be relevant for the different categories of transmission systems. The evidence that appropriate measures are implemented, considering the category of transmission system in question and the threats considered relevant for that category of transmission system, shall be documented in the Safety Case for the signalling system. The threats relevant to be considered are also cyber threats for category 3 transmission systems. EN 50159 (2010) further covers cyber security only in terms of intentional attacks by means of messages to safety-related applications. Issues concerning confidentiality of safety-related information and preventing overload of transmission system is not covered by EN 50159 (2010).

The authors of this paper have experience as independent safety assessor in projects where the relevant requirements related to cyber security have been touched upon. According to our experience, the transmission system (communication network) will be shared between different signalling-system applications. One practical solution related to this would be to produce documentation for the transmission system (including assessment of this set of documentation) that could be re-used in the Safety Cases for the different signalling systems. The result of this approach could be application conditions that must be respected by the signalling systems and documented being handled in each signalling system's Safety Case. An issue to further consider in this matter, is how static the set of documentation, or the assessment of such, for the transmission system can be, considering the changing cyber threat landscape.

As can be seen from the discussion above related to the requirements from EN 50129 (2018) and EN 50159 (2010), cyber security is already today an important aspect in safety approval of railway signalling systems.

3.1 *Cyber security related to communication systems*

For safety related electronic systems that involve the transfer of information between different locations, the transmission system forms an integral part of the safety-related systems, and it must be shown that the end-to-end communication is secured in accordance with the railway safety standard. The required documentation must be included in or referenced by the Safety Case for the safety related electronic system. As part of ensuring that the end-to-end communication is safe, cyber security related threats may be handled, depending on the category of the transmission system that are applied. The transmission system which serves the transfer of information between different locations, has in general no preconditions to satisfy, and is from a safety point of view either not trusted, or not fully trusted. EN 50159 (2010) describes possible configurations of the safety related communication in transmission systems. The standard divides the safety related communication into:

- safety related functions (to ensure authenticity, integrity, timeliness, and sequence of data) that are implemented in the safety-related equipment, and
- safety-related cryptographic techniques which protect the safety-related messages. These techniques may either be implemented in the safety-related equipment or outside the safety-related equipment but checked by safety techniques. In our view, the latter case might to a larger degree facilitate issuing a cyber security case, as described in the next section of this paper.
- Non-safety-related transmission system which may include protection functions and/or access protection functions. In our view, implementation of the protection functions and/or access protection functions may be documented in a cyber security case, as described in the next section of this paper.

Concerning cyber security related threats, EN 50159 (2010) only addresses protection against possible threats arising from unauthorised users, thereby excluding intentional or unintentional misuse from authorised users. Having this in mind, cyber threats originating from unauthorised access are present for category 2 and 3 transmission systems only. Category 1 transmission systems are characterised by being under the control of the designer and fixed during their lifetime. As such there are no risk of unauthorised access for category 1 transmission systems and therefore no cyber threats arising from unauthorized access. Examples of category 1 transmission systems are air gap transmission from track balise to train antenna, proprietary serial bus internal to the safety related system, and industry-standard LAN. Concerning category 2 transmission system, which is considered as an open transmission system, possible cyber threats are handled by the transmission system itself, since the requirement for claiming category 2 is that the risk of unauthorised access to the transmission system is negligible. Risk evaluations should demonstrate that the risk is negligible. Examples of potential category 2 transmission systems are WAN belonging to the railway, switched circuit in public telephone network, leased permanent point-to-point circuit in public telecom network, etc. A category 3 transmission system is considered an open transmission system for which a significant opportunity for unauthorised access is present. Examples of category 3 transmission systems can be packet switched data in public telephone network, internet, circuit switched data radio (e.g., GSM-R), packet

switched data radio, WLAN, etc. Concerning safety related systems communicating through category 3 transmission systems, defences are required to be implemented to mitigate cyber threats. In this context, an example of such could be masquerade messages. Cryptographic techniques are potential types of defences to mitigate these threats. In comparison, for category 2 transmission systems defences are not required to be implemented to the same degree by the safety related functions to mitigate cyber threats arising from unauthorised access. This is because the transmission system itself has implemented mechanisms for preventing unauthorised access.

4. Coming railway regulation on cyber security in EU

The recent ENISA study (ENISA, 2020) regards the level of implementation of cyber security measures in the railway sector within the context of enforcement of the high-level NIS Directive (EU Parliament, 2016). Under the NIS Directive, operators of essential services will have to take appropriate security measures and notify serious cyber incidents to the relevant national authorities. The ENISA study was based on a survey addressing cyber security among operators of essential railway services in the European countries. The report presents a thorough list of essential railway services accompanied by a high-level overview of the railway systems they support. One major finding was that EU member states have chosen different approaches to the NIS Directive implementation, although all highlighting the transport sector as essential.

The ENISA study also takes a special look into the European Railway Traffic Management System (ERTMS) with key cyber security recommendations. The European Union Agency for Railways (ERA) plays the role of system authority for the ERTMS implementation. As a standardised solution within control, command, and signalling (CCS), ERTMS has high availability and safety integrity requirements. Cyber security reflects on safety functions, as well as availability and integrity requirements of the embedded ICT systems (operational).

At the standardization front, CENELEC's TC9X WG26 "Electrical and electronic applications for railways" is currently finalising the European technical specification CLC/FprTS 50701 (2021), introducing requirements as well as recommendations for cyber security within the railway sector (CENELEC, 2021). The purpose of this standard is stated as: "*when a railway system is compliant to TS 50701, it can be demonstrated that this system is at the state of the art in terms of cyber security, that fulfils its targeted Security Level (SL-T) and that its security is maintained during its operation and maintenance*". The technical specification provides guidance on how cyber security could be managed in the context of the EN 50126-1 (2017) RAMS-lifecycles. In short, the TS intends to:

- be compatible and consistent with EN 50126-1 when it is applied to the System under Consideration (SuC),
- separate the safety approval and cyber security acceptance as much as possible due to the lifecycle differences between safety and cyber security, and
- identify necessary synchronization steps related to cyber security between the system integrator (company bringing together subsystems into a whole) and the asset owner.

The security models, concepts and risk assessment described in CLC/FprTS 50701, here TS 50701 (2021) are based on the IEC EN 62443-3-2 (2020). It is consistent with the application of security management requirements described in EN ISO/IEC 27001 (2013) and EN ISO/IEC 27002 (2013). Cyber security in context of TS 50701 is to protect the railway systems' essential functions in case they are threatened by malicious cyber attackers. Essential functions are capabilities required to maintain health, safety, and environment, as well as availability for the SuC. At the start, the system operator should establish a high-level railway zone model according to IEC EN 62443-3-2 (2020) for SuC id. and initial risk assessment.

TS 50701 (2021) allocates specific cyber security activities with synchronization and corresponding deliverables along the lifecycle phases of EN 50126-1 (2017). These activities involve coordination between the stakeholders' system engineering, Safety, RAM-, Verification and Validation, Testing- and Commissioning activities. Here, it is worth mentioning that continuous operation is one of the primary goals of security in contrast to the domain of functional safety. Losses of availability for trains or railway networks might in some cases for safety reasons be considered a safe state in the scope of functional safety. As part of the coordination, it is advised to separate the cyber security and safety issues as far as possible and coordinate them adequately to decouple the safety approval and cyber-security assurance processes.

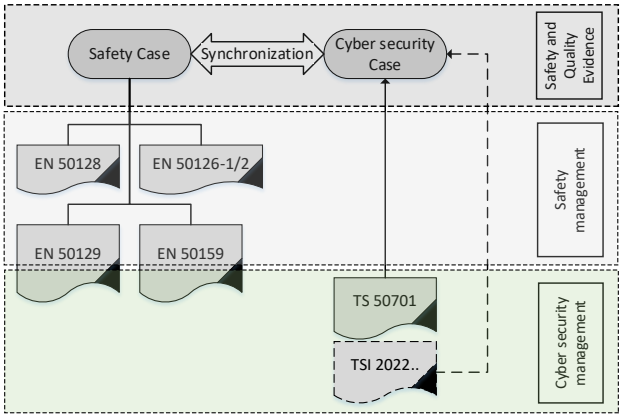

Fig. 2. Safety Case and Cyber security Case interaction

One suggestion in TS 50701, to achieve the necessary levels of separation and coordination, is to define only a limited number of coordinated cyber security objectives to be implemented with the cyber security case. Fig. 2, here illustrates the interaction and synchronization between the Safety Case and Cyber security Case including the relevant regulations. Definition of the cyber security requirements specification in RAMS life cycle phase 3 is based on the detailed risk assessment. Risk assessment is performed for each zone, or cluster of zones and conduits according to IEC EN 62443-3-2 (2020).

Risk-acceptance principles follow the principles of CSM-RA (EU, 2013):

(i) Application of Codes of Practice
(ii) Analysis of similarity with Reference Systems
(iii) Explicit Risk Evaluation

If explicit risk evaluation applies, the task is to derive appropriate SL-T vectors and allocate countermeasures for the remaining threats. According to IEC EN 62443-3-3 (2019), cyber security requirements are grouped into seven classes, which form a basis for the SL-T vector:

(i) Identification and authentication control (IAC)
(ii) Use control (UC)
(iii) System integrity (SI)
(iv) Data confidentiality (DC)
(v) Restricted data flow (RDF)
(vi) Timely response to events (TRE)
(vii) Resource availability (RA)

The fulfilment of the (high-level) cyber security objectives is demonstrated in a Cyber security Case. In practice, the objectives are fulfilled by the cyber security functions, and with so-called Security Related Application Conditions (SecRAC, like SRAC for safety). If the cyber security functions are changed, it must be demonstrated that the safety-related cyber security objectives still hold (including the SecRACs).

For safety approval, frequent changes should be avoided because of the comprehensive and costly safety demonstration. On the other hand, for cyber security reasons frequent updates should be easy in order to patch the system in time. Therefore, there is a trend to segregate cyber security from safety as much as possible. As a result of the above documentation structure, the essential safety documentation can be maintained as the cyber security process adapt to changing threat scenarios.

The process of cyber-security assurance and system acceptance for operation involve three types of activities according to TS 50701: 1) Verification, 2) Validation, and 3) System acceptance. The Cyber security Case (Fig. 3) contains all assurance evidence of the verification and validation activities for the SuC and addresses any remaining open issues by SecRACs.

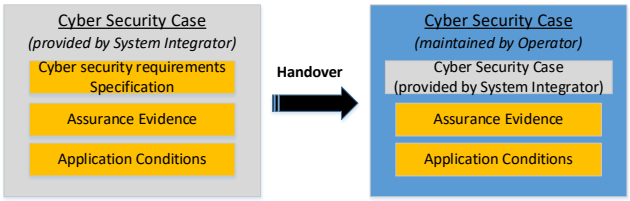

Fig. 3. Cyber security Case (adapt. from CLC/FprTS 50701)

The Cyber security Case provided by the System Integrator is updated once the SuC has been validated for its intended use. If proven successful, the railway operator accepts the updated Cyber security Case during the SuC Handover as illustrated in Fig. 3. The Cyber security Case of the railway operator can refer to several Cyber security Cases from different System Integrators as indicated by the grey colour box to the right in Fig. 3.

When it comes to operational, maintenance and disposal requirements, TS 50701 provides advice for vulnerability management and patch management activities. Here, security patch impacting safety functions shall be coordinated with the safety management and proved in the Safety Case. In future versions of TS 50701, activities like security monitoring, incident management, business continuity and crisis management are announced.

5. Discussion on cyber security in railway

This section discusses major findings from the former sections starting with the brief literature review. Then possible impacts of cyber security aspects in current, and upcoming regulations are elaborated. Pros and cons of the concept Cyber security Case is outlined. Suggestions, or possible improvements are finally discussed, mainly related to regulation and the common safety approval processes. We elaborate on basis of our own experience as safety assessor within the current safety legislation in Norway. This outline reflects only the authors' views.

5.1. *Major vulnerability threats and vulnerabilities*

From the literature review in Section 2, some implications of cyber threats to the safety assessment and safety documentation were outlined. The importance of learning from accidents and identifying deficiencies in early design of railway control systems was shown. Trade-off between available resources and security in the design process often becomes an issue. The method of Levshun et al. (2020) is here a contribution that combines elements of design and verification techniques through a seven-stage model supporting the design process. This kind of verification provides a check that the system is secured against attackers of certain types at each stage of the model.

When it comes to analysis methods to capture effect of cyber threats to safety functions, the methods of Pizzi (2020) and Cormier & Ng (2020) were found promising. As a part of the threat- and vulnerability description, a common taxonomy is certainly important for stakeholders in understanding and communicating among each other. Of interest for the cyber security domain are the categories of *accidental acts or faults* and *malicious acts.*

5.2. *Status and discussion of railway regulation*

As indicated, there is high activity and interest connected to handling of cyber security in railway. However, we observe a bit of a wait-and-see attitude among stakeholders on how to act at present time. In that respect, ERA has also announced Technical Specifications of Interoperability (TSIs) on cyber security design of railway subsystems.

5.2.1. TS 50701 towards an EN 50701?

It seems like CLC/FprTS 50701 will be approved and issued as a final TS 50701 in mid-2021. It will become a guidance document that authorities in EU member states could refer to as the proper cyber security management in context of EN 50126-1 (2017). It may also turn out being a

European Norm in 2-3 years (EN 50701). A breeding ground for various practices or applications among the EU-member states may be one challenge until TS 50701 becomes a normative standard. The coming TSIs for sub-systems (e.g., TSI 2022 for CCS) will provide technical requirements to cyber security solutions that may overcome such variations and maintain interoperability.

5.2.2. The Cyber security Case - EN 50129 and EN 50159

As seen in CLC/FprTS 50701, separation of the cyber-security and safety processes might be a premise for the coming regulation and introduction of the Cyber security Case. As e.g., the relation between EN 50129 (2018) and EN 50159 (2010) is defined, the scope of these standards clearly differentiates the safety related equipment and non-safety related equipment. Design of railway systems in the future may to a larger extent follow these principles. However, we also observe arguments for an integration of safety and security as in e.g., Lundteigen & Gran (2019), related to the petroleum- and process industry. Benefits of a separation strategy in railway might be as follows:

- Making only a few overall cyber security goals in the Cyber security Case makes it easier to keep essential work processes separate and still maintain safety.
- Cyber-security defences are to a greater extent implemented in components outside safety-related equipment, and do not need to be in the Safety Case.
- Safety approval process can be managed slightly unaffected, at a level "as is" in terms of work and cost.
- The responsibility for cyber security is to a greater extent placed at the system-integrator and supplier levels compared to the asset owner, which is more the case when it comes to functional safety.

5.2.3. Synchronization between safety and security

Positive effects of minimizing number of synchronization points between safety and security processes in projects is the limited need for, or level of integration of different topics. This again will minimize the complexity of work and need for internal coordination during the project. Most truly, it improves working culture, as well as quality and motivation within both disciplines. Possible challenges with the Cyber security Case and synchronization are:

- Different time windows and duration of safety approval processes compared to the cyber security assurance that could make synchronization of activities more difficult (at GP-, GA-, and SA-level).
- SuC (System under Consideration) usually covers wider or goes beyond DoS (Definition of System) in the Safety Case. This fact might be challenging with respect to define exact interface with safety functions.
- If cyber security issues to a large degree are planned to be solved at SA-level, greater effort must be put on system architecture from the early beginning of.
- Coordination of the safety and cyber-security activities can be demanding in some projects. Security risk assessment must be consistent with the safety analysis in early project phases as basis for requirement specifications. Selection of the proper security design, which typically is finalised later in the process, will involve changes with possible impact on safety that could be overlooked.

5.3. *Status and discussion of safety approval process*

Given the regulations that will soon come into force, there will be a coming discussion regarding enforcement, responsibilities, and roles, as well as establishing good practices within the regulations. The following subsections discuss some aspects of these topics.

5.3.1. Cyber security handling based on new regulations

EN 50129 (2018) requires that cyber-security threats are managed during risk assessment and hazard control if an impact of cyber-security on functional safety is reasonably foreseeable and cannot be excluded by simple arguments. In that sense cyber security is already covered within the current standards and regulation. It is noted, however, that there are projects ongoing that are still based on the preceding version of the standard, EN 50129 (2003), that do not include requirements related to cyber security. The preceding version of the EN 50129 standard (2003), will be withdrawn in 2021-11-23 and it is from then on expected that a larger emphasis will be put on cyber security as part of the safety approval process.

The Norwegian Railway Authority (NRA) expects that TS 50701 when issued will be assessed carefully in Norway. The Norwegian Railway Administration, the railway companies and suppliers truly will begin to adapt to the standard. According to ERA, however, TS 50701 will be referred to in the Application guide for coming TSIs as voluntary. The NRA believes that regardless of the standard, the National Security Act in Norway (Ministry of Justice and Public Security, 2019) even today set requirements to cyber security in railway as part of the important infrastructures. In that respect, TS 50701 might provide guidance, or a recommended practice.

5.3.2. Responsibilities and roles including an assessor

CLC/FprTS 50701 highlight the stakeholders responsible for system engineering, Safety, RAM, V&V as well as testing and commissioning. The following discusses a possible new role of a third party, or role of an Independent Cybersecurity Assessor (ICybA) as support to the authorities in protecting safety, availability and HSE from cyber threats. Possible implications to existing roles as ISA- and NoBo assessment is also discussed.

Regarding independent assessments in connection with cyber security assurance, CLC/FprTS 50701 states: *If an independent cyber security system assessment is required or other regulatory requirements call for cyber security system assessment to be performed independently, an entity shall be appointed and be given authority to perform the independent security assessment of the SuC.*

The cyber-security assurance, as proposed in CLC/FprTS 50701, is handled in collaboration between actors like the system integrator, suppliers, and the system owner (e.g., the railway operator). The authors believe, however, on the following benefits with an ICybA as an independent actor in this regime:

- More thorough and independent assessment of cyber security is expected that strengthens the evidence of SL-T achievement.
- Greater value/benefit of periodic audits, e.g., related to the specific RAMS life-cycle phases on the topic of cyber security, as a follow-up of initial audits.

Possible disadvantages of engaging an assessor (ICybA):

- There may be more extensive work processes, and costs accumulating for cyber-security assurance in addition to the safety approval.
- Less flexibility in projects, possibility of delays if such an assessor is to be involved and needs to consider "every" change before implementation.

As mentioned, a possible solution may be to let an assessor carry out periodic audits, in which changes are captured (both the planned changes, and changes made). At the beginning of the project, the ICybA may assess the system integrators' change process, the process of doing impact analysis, updating design documentation, and how tests are conducted with the certain stakeholder roles involved. One more obvious need is also to consider involving the Independent Safety Assessor (ISA) when cyber-security objectives change that are prerequisite for safety.

6. Conclusion

Based on the initial literature review, a discussion has been started regarding the railway safety approval and how to cover cyber security aspects. Both the existing and coming regulations and standards to incorporate cyber security are discussed. The authors elaborate on challenges related to handling of cyber security considering the new regulations and standards. The important work in assuring cyber security has started from different perspectives and angles. As pointed out, effective synchronization against the safety domain needs special attention. Some pros and cons of an independent cyber security assessment is also outlined in that respect. The possible use of an Independent Cybersecurity Assessor (ICybA) here needs to be clarified.

Acknowledgement

This paper has been written in connection with a strategic research project in SINTEF concerning cyber security effects on railway approval processes. The authors gratefully acknowledge the opportunity given for valuable discussions among colleagues at SINTEF Digital.

References

Adithya, T., Mustafa, A., Ravdeep, K., Ramin, K. (2019). Cyber security for eMaintenance in railway infrastructure: risks and consequences, *International Journal of System Assurance Engineering and Management, Vol. 10*, 149–159.

Beecroft, M. (2019). The future security of travel by public transport: A review of evidence, *Research in Transportation Business & Management*.

Cormier, A., Ng, C. (2020). Integrating cyber security in hazard and risk analyses, *Journal of Loss Prevention in the Process Industries. Vol 64*, 104044.

Dimitra, L., Theocharidou, M., Naydenov, R. (2020). Railway Cybersecurity - Security measures in the Railway Transport Sector. An ENISA study report, November 2020.

Gabriel, A. et al (2018). Cyber security flaws and deficiencies in the European Rail Traffic Management System towards cyber-attacks, *Cybersecurity Issues and Innovations for Crisis Response Proceedings of the 15th ISCRAM Conference – Rochester, NY, USA May 2018*

Gina, T., Kesan, J., Linfeng, Z., Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure, *Elsevier, Transport Policy, Volume 79*, 103-11.

Kertis, T., Prochazkova, D. (2018). Impacts of lacks in design of control systems in rail transportation, *Smart Cities Symposium*, Prague.

Levshun, D., Kotenkoa, I., Chechulin, A. (2020). The application of the methodology for secure cyber–physical systems design to improve the semi-natural model of the railway infrastructure, *Microprocessors and Microsystems*, Elsevier.

Lévy-Bencheton, C., Darra, E. (2015). Cyber security and resilience of intelligent public transport: Good practices and recommendations. Technical report, ENISA.

Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A. (2006). Safety vs. Security, *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (PSAM-8)*, New Orleans, Louisiana, USA.

Liveri, D., Theocharidou, M., Naydenov, R., (2020). Railway Cyber security – Security measures in the Railway Transport Sector, *ENISA Technical Report*. ISBN: 978-92-9204-412-1.

Lundteigen, M.A., Gran, B.A. (2019). The need of improved methods to handle functional safety and cybersecurity in industrial control and safety systems, *Researchgate.net.*

Pawlik, M. (2019). Concept of the railway safety, security and cyber security functional integrity levels, *Open Access, MATEC Web of Conferences Vol. 294, 03003.*

Pizzi, G. (2020). Cyber security and its integration with safety for transport systems: not a formal fulfilment but an actual commitment, *Transportation Research Procedia. Vol. 45*, 250-257.

Rekik, M., Gransart, C., Berbineau, M. (2018a). Analysis of Security Threats and Vulnerabilities for Train Control and Monitoring Systems, *2018 15th International Multi-Conference on Systems, Signals & Devices (SSD)*, 693-698.

Rekik, M., Gransart, C., Berbineau, M. (2018b). Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems, *IEEE CNS 2018 - 1st International Workshop on System Security and Vulnerability (SSV).*

Śliwiński, M. (2018). Safety integrity level verification for safety-related functions with security aspects, *Process Safety and Environmental Protection. Vol 118*, 79-92.

CLC/FprTS 50701. Railway applications - Cyber security, TC9X-Working Group 26. CENELEC (2021).

ENISA (2016a). Threat taxonomy: A tool for structuring threat information. Technical report, ENISA.

ENISA (2016b). Cyber security and resilience of smart cars: Good practices and recommendations. Technical report, ENISA.

EU Parliament (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union.*

EU Commission (2013). Commission Implementing Regulation (EU) No 402/2013 – on the common safety method for risk evaluation and assessment. *Official Journal of the European Union.*

Ministery of Justice and Public Security (2019). *"Lov om nasjonal sikkerhet", (Eng. The Security Act.).* Lovdata.