Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P210-cd

Cybersecurity in railway - alternatives of independent assessors' involvement in cybersecurity assurance

Eivind Halvard Okstad

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

Robert Bains

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

Abera Hailu Mewcha

Sporveien, Norway. E-mail: Abera.hailu.mewcha@sporveien.no

Lars Halvdan Flå

SINTEF Digital, Norway. E-mail: lars.flaa@sintef.no

Karin Bernsmed

SINTEF Digital, Norway. E-mail: Karin.bernsmed@sintef.no

Cybersecurity and related security management become important issues in railway projects and operations when implementing new digitalised technology. The railway industry is facing an increasing degree of digitalisation like else in society. CENELEC issued the CLC/TS 50701 in 2021 that may become the most important basis for the railway actors to manage railway cybersecurity in context of the RAMS lifecycle processes. By connecting cybersecurity to the railway application lifecycles, CLC/TS 50701 supports the identification of system requirements related to cybersecurity, and preparation of the associated documentation for security assurance and system acceptance. Like the role of an independent safety assessor acting in the safety domain of railway, the authors believe in, and suggest an independent cybersecurity assessor to be involved in system assurance and acceptance with regards to cybersecurity. This paper presents alternatives to such involvement of an assessor and discusses the possible advantages and disadvantages of alternatives based on a set of parameters and criteria. Recommendations with respect to involvement are fully based on qualitative evaluations of the mentioned criteria. Preliminary results are derived from discussions among SINTEF researchers, as well as discussions with actors from the railway industry. The alternatives have been balanced and validated against findings in the literature, that also covered approaches seen in other industrial domains.

Keywords: Cybersecurity, Security management, System assurance, Verification, Railway

1. Introduction

As railway transportation becomes a critical infrastructure in most of the European countries, modernization and development will continue for years to come. Projects are facing increasing use of new technology and digitalisation. In addition to technical safety and availability requirements (RAMS), digitalised systems need protection when affected by cyber threats, i.e., maintaining the cybersecurity.

According to the new technical specification CLC/TS 50701 (CENELEC, 2021) it is advisable to separate cyber-security and safety issues as far as possible and coordinate them adequately to efficiently manage domain specific lifecycle activities and approval processes. Otherwise, each change affecting the security of the system may trigger a new safety approval. There is no specific requirement to an independent cybersecurity assessor (ICA) in CLC/TS 50701. However, the authors believe there are benefits of involving such an assessor. An independent assessment body may be appointed by national authorities and given authority to perform independent security assessment of railway systems (CENELEC, 2021). The cybersecurity assessor shall be independent from the project manager, and a different entity to those having other roles in the project.

Based on this, the authors would like to address different alternatives to involvement of an ICA and conclude at some recommendations.

1.1. *Background*

According to ENISA (2021), the European railway undertakings (RU) and infrastructure managers (IM) need to address cyber risks to railway systems as part of the security risk management processes. Management of cybersecurity related to critical infrastructures was first emphasised through the Network and Information Security (NIS) Directive that came into force in 2016 (EU Parliament, 2016). For OT-systems (operational technology) that are most relevant in railway, important frameworks are the industry standards: ISA/IEC 62443 series, CLC/TS 50701, and the recommendations of the Shift2Rail project: X2Rail-3. The technical specification CLC/TS 50701 introduces cybersecurity requirements to railway applications, and it adopts the basic cyber-risk management principles found in ISA/IEC 62443. The document applies to communications, signalling and processing domains (CCS), to rolling stock (RST) and fixed installations domains of railway systems.

CLC/TS 50701 provides guidance and specifications on how cybersecurity will be managed in the context of EN 50126-1 RAMS lifecycle process. These security activities need to be synchronized with the RAMS process and involve coordination between stakeholders' system engineering, Safety, RAM-, Verification and Validation, Testing- and Commissioning activities (see Figure 1).

It is worth mentioning that continuous operation is one of the primary goals of cybersecurity in contrast to the domain of functional safety that is treated more statically at project milestones (Okstad, et al., 2021).

Work is going on in the European Union and member countries to adapt cybersecurity practices to the CLC/TS 50701 (CENELEC, 2021). Guidelines are produced, and research and development activities are going on in parallel. One example is the guideline of building zones and conduits for a railway system (ENISA, 2022).

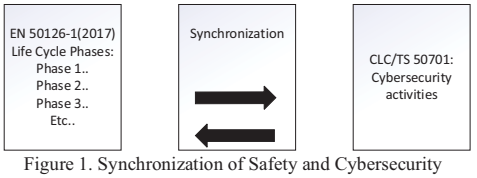

Figure 1. Synchronization of Safety and Cybersecurity

In Norway, there are still no requirements to involve an assessor, or an independent third party from the national authority's point of view. Therefore, it is a current issue to identify advantages and disadvantages of involving such an assessor in railway cybersecurity assurance. The present article argues for alternative levels of involvement of an independent assessor in system assurance with respect to cybersecurity requirements. Following a brief literature study, a comparative evaluation of alternative approaches to assessor involvement is presented. During the work, railway companies have been contacted and allowed to share their experiences with the research team. Typical information was concerning treatment of cybersecurity issues, and handling of related requirements in projects and when systems are put in operation. Then next, how was the company's opinion with regards to a possible role- and kind of involvement of an assessor in the cybersecurity assurance process.

2. Study approach

This work is based on a multidisciplinary collaboration between SINTEF researchers with background from generic cybersecurity, safety research, and assessors in the railway domain. In addition, practical experience from the railway sector is added. A combination of literature review, internal and external meetings as well as workshops have been used in preparing the input information, analysis and synthesis of results and recommendations from the study. The study approach can be described in four steps:

1. Literature study: To check out practices for the involvement of an independent party in other domains (oil and gas, maritime etc). Are there publications in general that look at the effect of independent third-party assessment of compliance with requirements? For example, find out if there is any research in psychology (sense of responsibility) in this area?

2. Definition of alternatives: To define options for a possible independent third-party involvement in conformity assessment of cybersecurity in railways. The proposed alternatives are to be assessed against findings in the literature study.

3. Comparative method: To develop a method for evaluation of the various alternatives. Advantages and disadvantages shall be assessed based on project parameters and criteria for usage in evaluation of the various alternatives. Values or scores are given to parameters based on an agreed scale, which is further justified in the discussion.

4. Comparative evaluation: To define the parameters and allocate values. This evaluation should be carried out by the research team in collaboration with the external actors from railway companies.

3. Literature review

A short literature review was conducted that covered practices (both established and recommended) related to the handling of cybersecurity within comparable industrial domains like the maritime-, aviation- and energy industry.

The information is presented as brief overviews, according to the authors impressions, from the different sources of the cybersecurity certification regimes and processes for cybersecurity assurance. Note, the collected information has not been verified outside the work with this paper. Typical information is type of activities, documentation, and involvement of independent third parties that appears to be representative of the domains.

3.1. *Cybersecurity certification in maritime*

The maritime domain has traditionally been referred to as less regulated than many of the other transport domains.

DNV has introduced a cyber secure class notation for vessels[a]. The class notation has three "levels": *cyber secure*, *cyber secure (essential)* and *cyber secure (advanced),* each implying different levels of risk reduction. *Cyber secure* is intended to meet the intention of the resolution on maritime cyber risk management in safety management systems (MSC.428(98))[b], from the International Maritime Organisation (IMO). *Essential* and *advanced* require compliance with DNV's security profiles 1 and 3, respectively. The security profiles are based on ISA/IEC 62443 Security Levels 1 and 3.

[a] DNV-CG-0325 Cyber secure, https://www.dnv.com/services/cyber-secure-class-notation-124600

[b] International Maritime Organization.https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

The International Association of Classification Societies (IACS), a membership organization and principal technical advisor of IMO, has adopted two new requirements for cyber security of ships (URE 26, URE 27). DNV has also created a procedure for cyber security type approval of systems and component that are to be installed on vessels[c]. The procedure is initiated when a manufacturer submits a request for type approval. DNV then reviews a set of required documents, provided by the manufacturer, and performs tests to verify security capabilities. Upon completion of these activities a certificate with a validity of 2 years is issued.

IMO decided that from 1 January 2021, an approved Safety Management System (SMS) should take cyber threats into account. IMO has therefore issued a set of guidelines on maritime cyber risk management (IMO, 2021), which provide high-level recommendations for maritime cyber risk management. These recommendations are intended to be incorporated into existing safety risk management processes. Note that an earlier version of these guidelines was adopted by the Maritime Safety Committee (2017) in the form of a resolution. An example of a recognised organization that can perform audits of maritime SMS is DNV[d].

3.2. *Cybersecurity certification in aviation*

Within aviation, the mandatory set of cybersecurity standards DO-326A (US version) and ED-202A (European version), which are used for airworthiness security certification have been adopted. These sets of standards were developed jointly by the European and American aviation industry, coordinated by the European Union Aviation Agency (EASA, 2014) and Federal Aviation Administration (FAA, 2014). Today, the standards apply to any certification of aircraft, rotorcraft, engines, and propellers. Stakeholders aiming to have their equipment airworthiness certified, will then apply for certification from the agencies where the aircraft has been registered. Both EASA and FAA are independent agencies, responsible for ensuring safety of all aspects of non-military aviation. Contrary to the maritime domain, which is less regulated, the operation of a civil aircraft without an airworthiness certificate is strictly prohibited.

In aviation, the independent agencies involvement in the assurance and certification process will vary, depending on the risk of non-compliance. As described in a Certification Memorandum issued by EASA in 2019[e], the risk of non-compliance is calculated as a combination of the likelihood of an unidentified non-compliance and the consequence in terms of the applicant's performance level. EASA's level of involvement will then vary from no verification at all of any of the compliance data (for low-risk products/systems) to the review of a large amount of compliance data, detailed interpretation of test results, and participation in a large number of compliance activities, such as witnessing of tests, audit, etc. (for high-risk products/systems). It is worth noting that the memorandum explicitly states that the risk-based approach to determining EASA's involvement in the certification process is applicable also to the assurance of cyber security aspects during the airworthiness certification process.

3.3. *Cybersecurity certification and assessment in the energy industry*

Leszczyna (2018) performed a review of standards and guidelines for security assessment of smart grid applied in the power industry, based on references found in the literature. The intention was to identify the standards that can be applied to security assessments of smart grid components. In this section we provide an overview based on this work. The six most frequent standards and/or guidelines in this context were:

- IEC 62351
- ISO 27000 series
- NISTIR 7628
- IEC 62443 series
- NERC CIP
- IEEE 1686

IEC 62351-1 relates to the process of assessing security requirements of assets. This should be a periodic process, unless political or technical changes make an immediate new assessment necessary.

ISO 27001, in control A.18.2.2, requires periodical checks to verify compliance with relevant policies and standards. This should be performed by managers. Else, Leszczyna also identified A.14.2.8 System security testing and A.18.2.3 Technical compliance review as controls that refer to security assessment, whereof the former typically include the involvement of independent experts.

NISTIR 7628 requires both the organization and the assessor to be represented in the security assessment. The role or attributes of the assessor is however not discussed further. Furthermore, the standard defines the objective of the assessment to verify that stated objectives are reached and it may therefore be wider than just ensuring compliance with requirements and regulations.

IEC 62443-4-1 (14.3.1) requires that a person should be appointed to assess the security achieved by a product. How this assessment should be carried out is not discussed.

NERC is the authority tasked with creating and enforcing compliance with reliability standards in North America (NERC, 2022a.). According to Leszczyna (2018), NERC CIP is comprised of 11 documents, all of which can be applied to compliance testing (NERC, 2022b.). In part

[c] DNV-CP-0231.

[d] DNV. Maritime cyber security. https://www.dnv.com/../maritime-cyber-security/index.html

[e] Certification Memorandum: Criteria for the determination of the EASA level of involvement in product certification. EASA CM No.: CM-21.A/21.B-001 Issue 01, issued 02 July 2019.

010-3, the enforcement authority is defined to be NERC, a regional entity or another entity designated by an applicable governmental authority.

IEEE 1686 does not include description of security assessments or methodology for security assessments.

3.4. *Norwegian and EU-regulations in energy industry*

The Norwegian Regulation on safety and emergency preparedness in the power supply system (NVE, 2022) requires the asset owner to ensure that suppliers comply with requirements for information security (§6.5). The contract shall ensure the right of the asset owner to perform audits. The asset owner can perform this audit themselves or by relying on an audit performed by a third party. Lastly, it is required that the asset owner performs audits of security measures at regular intervals (§6.9).

In their publication on subject: Smart Grid certification in Europe, ENISA discusses challenges to smart grid certification and outlines what they perceive to be an ideal smart grid certification scheme (Baars, et al. 2014). The main challenges to a smart grid certification scheme are identified to be the different approaches used in different member states and the lack of an EU body providing guidance. Three recommendations for implementing a certification scheme are highlighted:

- Harmonized practices: Common EU practices should exist but allow for specific elements required by different national certification schemes. National schemes will be confirmed by EU accreditation bodies.
- Member states should have the possibility to amend or expand on European requirement to support use cases specific to each member state.
- An EU steering committee: This committee should have oversight on smart grid certification, European security requirements, and the development of national certification schemes.

The document outlines three assessment levels, consisting of first-, second- and third-party assessment. The choice of assessment level can be tied to the level of risk posed by non-conformity or to the criticality of components. However, somewhat contrary to this, the document claims that in practice only third-party assessments are seen as trustworthy and this is therefore recommended.

The connection between levels of risk and assessment levels is not thoroughly discussed. The use of the Smart Grid Information Security framework is advocated to determine the level of risk of smart grid use cases. Based on this, certification can be focused on the components with the highest risk impact. Although the explanation focuses on what to certify, perhaps a similar solution can be used to determine who should certify.

Cost is not explicitly mentioned as a barrier to third-party assessments, but cost is mentioned in relation to assessment and certification. Lack of harmonization between member states is claimed to be a reason for increase in costs. Furthermore, keeping costs low is a challenge since security is relevant to many aspects of a systems and hence must be widely implemented. A potential remedy for high costs is suggested in the form of self-assessment tools. These can be used by vendors in a pre-assessment phase or during development.

3.5. *EU-regulation on cybersecurity*

The topic of cybersecurity certification has recently received attention at the EU level with the Cyber Security Act (European Parliament, 2019). The act establishes the European cybersecurity certification framework, which among others is to enable a harmonised approach at EU level to European cybersecurity certification schemes with a view to create a digital single market for ICT products, services, and processes (EUR-lex, 2022). According to the Horizon 2020 research program SPEAR, the Cyber Security Act permits both self-assessment and third-party assessment (SPEAR, 2022). Third party assessment shall be conducted by a conformity assessment body, who will conduct assessment activities (e.g., design review, penetration testing, source code review) to decide if certification is to be granted.

3.6. *IT-security in railway*

Safety approval of railway signalling systems are today based on among others the CENELEC standards EN 50126-1/2 (2017), EN 50128 (2011), EN 50129 (2018) and EN 50159 (2010). The main emphasis of the approval is on safety, although, cyber security, or IT-security as mentioned in the CENELEC standards for railway, are also addressed (Okstad, et al., 2021). EN 50129 (2018) and EN 50159 (2010) include requirements related to cyber security in the context of operational technology or (OT).

4. Evaluation of alternatives regarding independent assessor's involvement

The following section presents alternatives of an independent cybersecurity assessor (ICA) involvement based on the authors point of view.

4.1. *Evaluation methodology*

A comparative approach for evaluation of alternative involvement of ICA has been suggested. The alternatives are illustrated in Figure 2 and described below. The methodological approach implies a set of parameters and decision criteria as means for the evaluation.

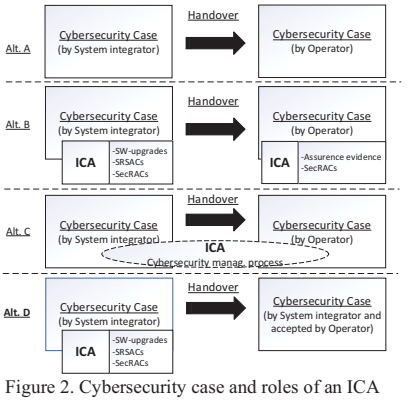

Figure 2. Cybersecurity case and roles of an ICA

The following four alternatives cover the basic needs:

A. No independent assessor. The Cybersecurity case is produced without any involvement of assessor.

B. Independent assessor assesses every planned change by client to a railway sub-system that could relate to:

   i. changes within requirement specification of the sub-system, or
   ii. SW-upgrades or improvements before implementation, and
   iii. conformance of the cybersecurity management process against agreed cybersecurity standards.

C. The independent assessor assesses only the clients' (System integrator and Operator) processes for handling cybersecurity. Spot-checks of the responsible entity for project execution are performed to check conformance to procedures and requirements. This kind of "audit" may cover generic processes that are valid across specific systems being developed.

D. The independent assessor assesses only the system integrator's Cybersecurity case if the operators doesn't develop an overall cybersecurity case. This might be the most common practice today.

Alternative B implies a cybersecurity case from both the system integrator and operator that documents the changes and cybersecurity assurance. The (general) process of handling cybersecurity incidents and vulnerabilities will also be focused on in this alternative, i.e., the quality management. Evaluation of changes may be based on:

- impact analysis of technical changes and/or framework conditions,
- updated vulnerability analyses, or
- updated cybersecurity risk analyses followed by changes in the cybersecurity requirements specification.

There may be conditions and/or variations within each alternative above but the authors consider A-D above to cover overall practices.

Alternative A might be the general practice for now in most of the rail industry and how the players see the issues with cyber security today. A cyber security case can be produced by the system integrators and system owners/operators with the underlying documentation, or something similar. Penetration tests that may be carried out by third parties are also done. But as mentioned, there is no requirement for an independent 3rd party involved in system assurance. Alternative C is nevertheless interesting, where the assessor assesses the processes and makes a note based on this. Option B is more like a 100% check with a cybersecurity case, comparable to ISA (Independent Safety Assessor) regarding Safety. Alternatives A and C appear to be the most common ways (or practical) of approaching cybersecurity in railway from an operational viewpoint.

Alternative B should include assessing the management process, but the time aspect may be challenging in an operational context. Therefore, alternative C might be the best alternative to B on general basis. Rail companies in Norway most likely follow options A or D today with no separate cybersecurity assessor involved, even though option D is not that recommended. The system integrator and operator or infrastructure manager should develop security cases within their own scope of work to ensure cyber secured environment. The authors believe that option-D projects anyway should benefit from including the use of an independent assessor (ICA).

Alternative D implies the operator doesn't develop any overall cybersecurity case by own. That means, only the system integrator develops cybersecurity case for the system including its interfaces. The operator might however, deal with security Application Conditions (AC) as indicated in Figure 2. To the extent that these ACs are safety-related, a distinction is made between the Safety-related Security Application Conditions (SRSACs), and SecRACs that are related to functionality only (Figure 3). It is the authors opinion that both the SRSAC and SecRAC could be documented in the Cybersecurity Case. In this way, a continuous update of the Cybersecurity Case (including measures) in case cyber issues occur means that unnecessary updates of the Safety Case are avoided. If not possible, the Safety Case need to be updated and trigger a new safety approval process. From the perspective of the railway industry, alternative D might be the most common approach dealing with cybersecurity today. Requirements in TS/CLC 50701 could be fulfilled anyhow given good coordination between the system integrator and operator.

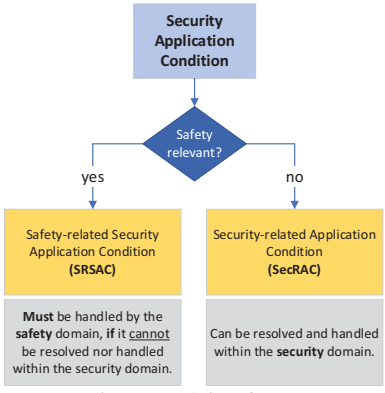

Figure 3. SRSACs and SecRACs (adapt. from CENELEC, 2020)

4.2. *Parameters and criteria*

As mentioned, selected parameters with a decision criterion, or a set of criteria are used to compare the alternatives against each other. Each criterion could attain the following qualitative scores:

- (-) Not recommended
- (+) Recommended
- (<+) Less than (+), and (>+) More than (+)
- (++) Highly recommended

Possible impact of a cyber-attack depends on which life cycle phase the system, or sub-system stays in.

For simplifying reasons, we only differ between the design phase (D) and system in operation (O) for the purpose of this method. The selected parameters/phase with criteria are as follows:

Table 1. Parameters and criteria to differentiate alternatives

No.	Parameter/phase (D/O)	Criteria (a, b, c, d)
1	Project cost or investment (D)	a. Development of system b. Minor changes to system c. Modification d. Major impact of cyber attack
2	Project duration/(D)	a. Within a year b. Multiyear project
3	Timespan of threats (D/O)	a. Time elapse between the need for a security update occur, and measures are implemented
4	Cybersec. risk (D/O)	a. Cyber risk after measure
5	Safety risk (D)	a. Safety risk after measure
6	Confidential. IT (D)	a. Business rated or admin.
7	OT- data (O)	a. Data from control systems
8	Quality of doc. (D)	a. Final documentation
9	Quality of syst. (D)	a. Final system 'as built'
10	Project org. (D/O)	a. Strong client organisation b. Hired from consultancy comp.

The evaluation applied the above parameters and was carried out in project meetings with researchers and representants from railway companies. Some assumptions were included in the evaluation as described in section 4.1. This simplified approach was chosen of practical reasons and the available time. There are more robust and comprehensive methods in literature like e.g., the Analytical Hierarch Process AHP for multi-criteria decision making (Golden, et al. 2012).

4.3. *Evaluation*

Table 2 below summarises the evaluation of each alternative by use of the above parameters and criteria.

Table 2. Evaluation results

No.	Parameter/phase (D/O)	Crit.	A	B	C	D
1	Project cost or investment (D)	a	-	++	+	+
		b	++	-	-	-
		c	-	+	+	+
		d	-	+	++	+
2	Project duration/(D)	a	-	+	++	+
		b	-	++	+	++
3	Timespan of threats (D/O)	a	-	+	++	+
4	Cybersec. risk (D/O)	a	-	++	+	++
5	Safety risk (D)	a	-	++	+	++
6	Confidential. IT (D)	a	++	-	+	-
7	OT- data (O)	a	-	++	+	-
8	Quality of doc. (D)	a	+	++	>+	+
9	Quality of syst. (D)	a	<+	++	>+	+
10	Project org. (D/O)	a	-	+	++	+
		b	-	++	+	++

4.4. *Summary and discussion of results*

The results from the evaluation are presented through the evaluation table above with the number of different scores given to the parameter categories. There could be different ways of interpreting the above results. Based on project experience some reflections are made based on the scores. By summing the number of (-), (+), and (++) for each alternative (A-D) we gain the following distribution:

- Alternative A: 11 (-), 2 (+ or <+), 2 (++)
- Alternative B: 2 (-), 5 (+), 8 (++)
- Alternative C: 1 (-), 10 (+ or >+), 4 (++)
- Alternative D: 3 (-), 8 (+), 4 (++)

Based on the above results, we may conclude alternative B seems to be the most recommendable from an assessor point of view. However, applying alternative B is also a question of cost/benefit and in that respect, we could rather argue for alternative C, also scoring more (+) and (++) in total. However, a distinction should be made between the context of a system development phase and a system already in operation.

In a development project we might have plenty of time, the system is designed and assessed in parallel regarding safety and security. One may have a software development team and an assessment team, but both teams with dedicated specialists who seek optimal implementations within reasonable limits.

In an operational situation, however, time is actual money. Truly, it is expensive to take systems out of operation for an upgrade. For example, transport buses must be hired for trains, as often done in Norway. Safety and security should be treated independently, as the intention in TS/CLC 50701 (CENELEC, 2021). An implementation of cyber security measures should, however, be good enough, or at least better than it was.

4.5. *Learning from the literature study*

From the literature review we observe that NISTIR 7628 seems to require an independent assessor to be represented in the security assessment. The specific role of such an assessor is still not described.

The publication from ENISA regarding Smart grid (Baars, et al. 2014) outlines three assessment levels, consisting of first-, second- and third-party assessment. The assessment level is then tied to the level of risk posed by non-conformity or to the criticality of components. However, at last the document claims that in practice only third-party assessments are seen as trustworthy regarding security certification and thus, recommended.

Lastly, and according to the research program SPEAR, the Cyber Security Act permits both self-assessment and third-party assessment (SPEAR, 2022). Third party assessment shall then be conducted by a conformity assessment body, who will conduct assessment activities (e.g., design review, penetration testing, source code review) to decide if certification is to be granted.

The overall impression is that regulations and practices still vary among different industrial domains, but the outcome depends much on possible safety impacts on society, or any third party.

5. Case: Signal application

A signalling system is covered by a Safety Case, assessed by an ISA – Independent Safety Assessor. An associated transmission network is covered by a Cybersecurity Case, assessed by a possible ICA. See Figure 4 for the situation.

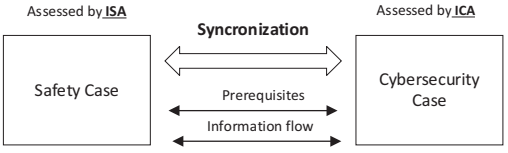

Figure 4. Assessment of a railway signalling system

The signalling system has prerequisites of a category 2 network according to EN 50159:2010/A1:2020. This entails a requirement that the risk of unauthorized access via the transmission network is negligible, i.e., this is a requirement from the Safety Case to the Cybersecurity Case.

The transmission network brings together several conditions that the signalling system must take care of to achieve secure communication. These Application conditions (or SRSACs) are information flow from the Cybersecurity Case to the Safety Case. Safety, as demonstrated in the Safety Case, depends among other things on the assumption of the category 2 network being maintained, and on the mentioned SRSACs.

As an example of operating situation: The transmission network needs an immediate upgrade due to a security incident has occurred. It is argued that the risk of unauthorized access is still negligible in the cybersecurity case, i.e., that the prerequisite set by the signalling system is still fulfilled. The SRSACs that the signalling system must comply with are thus, unchanged. An important question is then: Will an update of the Safety Case be required followed by an updated ISA report? As argued in section 4.1, this might be handled by the Cybersecurity Case.

Seen from an operational point of view, if such an upgrade is needed, there will also be a trade-off between how long the system will be out of operation (expenses) and what ambition the update has. A solution to this could be to do the update in two 'Steps':

1. The incident is quickly analysed to get an overview of the problem: Quick countermeasures (if possible) are implemented, and a simple validation is carried out before commissioning. The system should at least be better or more robust than before.

2. Then, while the system is running a more thorough analysis is performed, countermeasures are updated if the thorough analysis indicates it, and a thorough validation is performed. Once the update is validated, the system is updated at a time that causes minimal operational disruption.

The above solution, of cause, depends on how big the impact of the SRSAC on safety is. If impact of the incident is assessed to be 'less significant', then the 2-step solution might work. If not, safety aspects may become more important than maintaining operations and trigger a full implementation, analysis, validation at first place.

Anyway, you might avoid having the system out of service for a longer time than necessary by this strategy. An ICA may be hired to conduct verification of the intermediate measure(s). The first 'minor change to the system' or update is in any case better than it was, the second update may have a wider scope and analyses any secondary effects and is implemented after a thorough validation. The disadvantage is the need for two updates, but this can be compensated for by a shorter total shutdown time and better perceived user quality in overall.

By applying the evaluation methodology outlined in sections 4.1 to 4.3, we see that alternative A is recommended for Step 1 above because it relates to a 'Minor changes to system'. When it comes to Step 2 that is more like a 'Modification', alternative B, C or D may be the recommended strategies of involving an ICA in that order.

6. Discussion

From the literature we notice the ENISA's report on Smart Grid Security Certification in Europe (Baars, et al., 2014) includes considerations related to common requirements between EU member states. Creating a baseline set of requirements that are recognized by all member states is claimed to be difficult. This is due to member states having widely different requirements and levels of security. Removing all these member specific requirements is either not considered feasible or desirable, as the 'ideal' certification schemes is described to be a combination of union wide baseline requirements amended by member specific requirements.

An advantage of more harmonized requirements appears to be reduced cost. A workshop from 2012 revealed that current certification schemes were considered expensive, partly due to the different certification schemes in different member states. Union wide baseline requirement shall potentially enable acceptance in one member state to also be valid in another member state. Related to this is the desired property that several actors should be able to provide certification services, to avoid monopoly. A single framework coordinator should keep oversight over the certification bodies to ensure quality.

There may be different emphasis and arguments on the table when discussing the role of an ICA for railway applications. This is natural seen from the different parties point of views, as e.g., researchers, assessment bodies and railway companies. The ICA-alternatives (A, B, C and D) are meant as 'educated suggestions' only and should cover a relatively broad range of cases. It is therefore natural to see whether it is possible to argue for alternatives based on experience as well as findings in the literature study. In any case, there should be support for one or more of the alternatives on this basis.

It is natural to consider the entire life cycle when looking at the cost of the alternatives. It implies from an early development phase through the operational phase. A minor

change to a subsystem in the railway domain can typically be a simple adaptation of an existing station area. To choose involvement of an assessor here, or not, may depend on to what extent the changes effect on safety through the cybersecurity functions.

When it comes to the parameter and criteria for project cost i.e., parameter No. 1 in Table 1, there is a clear distinction in the recommendations regarding criterium (1): Development of system, and (2-4) which relate to a system in operation. For the latter, it often implies taking the system out of operation for a shorter or longer time, which again, leads to higher costs for the society.

The possibility of cybersecurity becoming part of the ISA scope can also be discussed. From the point of view of an assessor organization, it seems convenient to adapt the existing safety approval regime and infrastructures (procedures) in a flexible way. The challenge may be to balance the safety and cybersecurity objectives accordingly against the project needs. From the point of view of a project organization, it may quite well depend on the RAMS- and cybersecurity competence in the line. The latter is valid for both vendors, system integrators and the railway undertaker. Two extreme cases stand out here:

1. A strong core organization, or line organization at the developer, supplier or in the operator's operating organization.
2. A project organization based on hired advisers and otherwise little expertise in the line.

Here, the effect of the choice between A, B, C or D could have different importance and/or impact. Alternative B (or C) and D may have greater value in the latter case. The discussion regarding the level of documentation and handling of SRSACs and CybSACs in the Cybersecurity Case is also relevant. Especially, if some of the SRSACs can't, of some reasons, be handled in the Cybersecurity Case and trigger a new update of Safety Case involving an ISA. The discussion about these matters continues among the railway industry actors, regulation agencies and in the research community. The preliminary results presented in this paper are meant as a contribution to this discussion. Further research will certainly go on in SINTEF and elsewhere regarding processes and best practices of handling railway cybersecurity, including the need for a third-party involvement (ICA).

7. Conclusion

This paper discusses involvement of an independent cybersecurity assessor (ICA) in cybersecurity assurance within the railway domain. The recommended type of involvement depends on the project types with respect to complexity and duration. It is also a matter of quality and safety assurance during the project lifecycles as well as the level of maintaining system availability in the operational phase if affected by cyber threats.

Another aspect is the level of competence and resources found in the project organisations. In case of lacking such, it might strengthen the cybersecurity assurance process by involving an ICA at a certain level. In general, involvement of an independent cybersecurity assessor seems appropriate for new long-lasting railway projects that involve significant investment costs to society. For projects or cases where digitalised sub-systems or components are difficult to separate from-, and become close interconnected with safety functions, an independent cybersecurity assessor should preferably be involved in cybersecurity assurance, maybe as an extension to the ISA.

Acknowledgement

The work with this paper was funded by an internal research project in SINTEF. The authors also like to acknowledge the opportunity for valuable discussions with rail operators and colleagues at SINTEF Digital.

References

Baars, H., Lassche, R., Massink, R., & Pille, H. (2014). Smart grid security certification in Europe - Challenges and recommendations. Technical report, ENISA.

CENELEC (2020). Cybersecurity standard for EU Railways, TS 50701. Presentation at Cybersenate – Feb. 2020. Secretary of TC 9X/WG 26.

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

EASA (2014). Eurocae ED 202 Airworthiness Security Process Specification. Issued 1 June 2014.

ENISA (2021). Reliability Cybersecurity, Good practices in cyber risk management. Technical report, ENISA.

ENISA (2022). Zoning and Conduits for Railways. 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 Parliament (2019). The Cybersecurity Act. Regulation (EU) 2019/881 on ENISA and on ICT-technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

EUR-lex (2022). EUR-lex. https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX:32019R0881.

FAA (2014). RTCA DO-326A Airworthiness Security Process Specification. Issued 6 August 2014.

IMO (2021). Guidelines on maritime cyber risk management. The International Maritime Organization. MSC-FAL.1/C3, Rev.1.

Leszczyna, R. (2018). Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*, 22, 70-87.

NERC (2022a.) https://nerc.com/AboutNERC/Pages/default.aspx

NERC (2022b.) https://nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.

NVE (2022). Regulation on safety and preparedness in the power supply (No: "Kraftforsyningsforskriften". https://Lovdata.no.

Okstad, E.H., Bains, R., Myklebust, T., Jaatun, M.G. (2021) Implications of Cyber Security to Safety Approval in Railway. *Proceedings of the 31th European Safety and Reliability Conference,* ESREL 2021*,* Dublin, Ireland.

Golden, B.L., Wasil, A., Harker, P.T. (2012) *The Analytic Hierarchy Process – Applications and Studies*. Ed.1, eBook ISBN: 978-3-642-50244-6, Springer Berlin, Heidelberg.

SPEAR (2022). SPEAR2020 https://spear2020.eu/News

The Maritime Safety Committee (2017). Maritime cyber risk management in safety management systems, Annex 10 Resolution MSC.428(98), adopted on 16 June 2017.