Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
©2022 ESREL2022 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R09-01-099-cd

Cybersecurity Design for Railway Products

Jan Prochazka

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic, E-mail: jpr@qma.cz
VUT, Purkynova 464, 61200 Brno, Czech Republic, japro2amseznam.cz

Petr Novobilsky

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic.

Dana Prochazkova

VUT, Purkynova 464, 61200 Brno, Czech Republic, prochdana7@seznam.cz

Svatoslav Valoušek

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic.

Rail is the backbone of transport critical infrastructure and it is inherently a complex system. Cybersecurity design requirements for railroad are significantly changing with its modernization in the field of communication and automation technologies. The article deals with the methodology of determining the cyber-security design of a product intended for railway infrastructure, which is based on the recommended standards. The application of methodology considers processes in the context of cyber-physical systems and through risk analysis, risk judgement and management. Methodology serves as tool of risk management for the selection of optimal measures, which fulfill requirements of security design with optimal costs and lead to improvement of train security.

Keywords: Cyber-physical system, railway, risk, cyber security, security design.

1. Introduction

Critical infrastructure performs the basic functions of the State. In the field of transport, it is supported by the railway. Railway safety is threatened both by external and internal harmful phenomena, as well as by the human factor, its faults and the way of organization in the field of design, construction and operation. The area of cybersecurity currently requires special attention ISO 27001 (2022), and organizations must take steps to protect their networks and systems from cyberattacks.

Cybersecurity design requirements for railroad are changing significantly with its modernization in the field of communication and automation technologies. The nature of the railway as a cyber-physical system is becoming more complex and the requirements for safety are increasing significantly. The cyber world has updated its procedures for creating security design with the IEC 62443 standard (2019). The communication safety of the railway was thus given a new tool in the form of the specification TS 50701 (2021), which builds on this standard.

The basis of risk management according to ISO 9000 (2015) standards requires the appro-priate identification of target safety requirements, i.e., safety design. Safety design must not only reliably ensure adequate safety but must also be achievable and sustainable. With the major changes that the railway infrastructure is undergoing in these years, it is also necessary to update the procedures for creating cybersecurity designs.

Important tools are, determining the context of the product within the system, the entire risk management (identification, analysis, evaluation, determination of measures, settlement), the process of selecting requirements, the safety design report. The article deals with the methodology of determining the cyber-security design of a product intended for railway infrastructure based on the mentioned standards and processes from the context in the systems, through risk analysis to the selection and fulfillment of requirements.

2. Knowledge on Background of Problem

Cyber-Physical Systems (CPS) are integrations of cybernetic and physical parts and processes. Properties and phenomena in cybernetic subsystem influence situation in physical subsystem and vice versa. CPS is specific type of System of Systems (SoS), an open system that consists of several open systems of different nature and various locations, which are interconnected to ensure certain operations and activities.

The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general- purpose computing. Moreover, physical components are qualitatively different from object-oriented software components. Standard abstractions based on usually used methods and threats do not work (Lee 2008).

The world changes dynamically and CPSs as critical infrastructure don't operate in a controlled environment as result. CPS need to be constructed robust to be able to adaptable to unexpected conditions and subsystem failures. Interactive complexity and tight connections between elements in CPS can lead to a critical situation due to system failure. Complexity not only creates new dangers, but also makes them harder to detect (Procházka, Procházková 2022).

In harmony with assertion (Schneier 2002), it is showed that ensuring the security and safety is a process in which measures are applied to the human security in variable conditions. The high degree of uncertainty (knowledge uncertainty) does not allow a satisfactory prediction of the behavior of a complex system of systems in conditions in which many disasters of internal and external arise and a human factor acts. From this reason, the railway protection and train protection are difficult.

Big roles play *limits and conditions*, which are a set of clearly defined conditions for which it is proven that the operation of the train system is safe. It is necessary to include program for safety in design that ensures:

- safety and functionality of all fittings that corresponds to their missions,
- identification, evaluation, elimination or regulation of potential risks at acceptable level for important installations, systems and their various parts,
- risk management, which includes all possible disasters with resources inside and outside the technical facility that cannot be eliminated,
- protection of personnel, people in the vicinity, environment, facilities and property,
- use of new materials or products and test techniques only in a way that is only associated with minimal risk,
- insertion of safety factors that ensure corrective measures that lead to improvement,
- consideration of all appropriate historical data.

3. Railways as a System of Systems

Transport systems, in which rail is of fundamental importance, belong to critical infrastructure. The publication (Procházka, Hošková-Mayerová, Procházková 2019) showed that in recent decades the cause of railway transport failures are natural disasters, technical defects, human errors, organizational deficiencies and cybernetic causes (errors in hardware or software, or in their interconnection); the specific feature is changeability of train risk due to train movement.

One of the reasons for the failure is the complexity of the railway, which consists of many subsystems and many different elements. Subsystems and elements can work separately and together, performing a completely unique task that is remote from the tasks of individual entities. According to the findings summarized in (Procházková 2017), two system features are important to them, namely interactive complexity and close connections.

Complex interactions are unplanned, unexpected, and mostly unknown sequences that are not immediately understandable. Therefore, interactive complexity and close connections between elements in a complex system can lead to a critical situation due to systemic failure.

The above facts mean that risk thus becomes a systemic feature. Security requirements are formulated at the level of the entire cyber-physical system and then through a descending process to the subsystems. Due to the complexity and high interconnectedness of the monitored objects, the systematic analysis of vulnerabilities and robustness with respect to failures is difficult, which is why simulation results are used.

The railway is a complex cyber-physical system. Semi-automatic and automatic control systems are used to a large extent during its control. The quality of the control depends on both the hardware and the software of the management systems. From the point of view of the safety of the protection of people, the railway and its surroundings, it is necessary to address the area of the cyber system and its interconnection with the physical system. A big role is played by the interconnection of information systems and systems that perform specific tasks (Procházka, Procházková 2022).

The security of the system must not be compromised with increasing information performance, and a secure system must be guaranteed for particularly important items in the case of critical infrastructure. The information security process consists in protecting important assets of a cyber (information) system so that the required level of availability, integrity and confidentiality is ensured for important information (Novobílský, Kertis, Procházková, Procházka 2016, Boss 2020).

These requests are often conflicting, e.g., by ensuring confidentiality we reduce availability and integrity, as well as time requirements for encoding and decoding, transmission, authentication, etc. To ensure high security, i.e., high information performance and security of cybernetic systems, process and project management approaches of the "Total Quality Management" (TQM) (Zairi 1991) type are applied, on which the methods used as well as international and European standards for management systems are based.

As research and practical experience show, the basis for the safety of each device is quality design. Some design errors are irreparable during operation, and it is necessary to apply a lot of organizational measures, the effectiveness of which is not as great as the quality ensured by the design measures (Prochazkova 2017). Therefore, even in the creation of products for rail transport that have a cyber- physical nature, security design plays a role.

4. Tools for Development of Cybersecurity Design

The use of new communication and management technologies leads to the emergence of new risks associated with them. These risks need to be addressed within cyber-physical systems. At the same time, new technologies provide us with tools and procedures to deal with these risks.

An example is the IEC 62443 (2019) standard, which contains a set of tools and procedures to ensure the cybersecurity of control systems in the development and use phase of the product, from the point of view of the system and individual parts. Based on this, there are a large number of new possibilities in the field of cybersecurity, which can be implemented with different levels of security. Their selection should, therefore, consider their efficiency and sustainability during the operation and economic costs.

In connection with the IEC 62443 standard, we can combine a suitable safety concept with a so-called security vector, or (cyber-)security design. Cybersecurity design values individual chapters of cybersecurity in relation to the system or product being addressed. Design determination is specific to different types of cyber-physical systems. For example, railway infrastructure has a number of its own technical standards that govern it. Many of these standards can also have an impact on the process of determining cybersecurity design. The basic rule is, therefore, the TS 50701 (2021) standard, which addresses cybersecurity on the railway.

The safety design methodology on which we rely is part of the V-cycle of the product according to EN 50126-1 (2017). Next, we will describe the methodology for determining the safety design that forms the left part of the V-cycle, Figure 1.

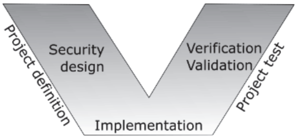

Fig. 1. V-cycle. Details are in (EN 50126-1 2018).

Standard IEC 62443 and standard EN 50126-1 are from different specialization and they differ in approach to problems. IT standards deals with confidentiality, integrity and availability of data or information. However, we need from them to deal with reliability, availability, maintainability and security (safety) to be applicable in railway infrastructure. IT security risk assessment has different assessment processes than as in RAMS (NIST SP 800-30).

The safety design of the train communication gateway after implementation is now subject to verification and validation, the right part of the V-cycle. This procedure is being implemented within the framework of the European COSMOS project (2021).

The basic prerequisite for the development of a methodology for determining safety design is the existence of quality management and risk management of processes in the company. The prepared methodology thus follows the procedures and measures established by the ISO 9000 standards (2015).

The main objective of the methodology is to determine the most appropriate safety design. The suitability of the design can be judged by various aspects. Many aspects are often specific to the place of implementation, such as knowledge, available technologies and their interconnectivity, etc. However, the main aspects tend to be the degree of risk reduction versus the cost of doing so, Figure 2. Optimization of the costs of securing the system on the railway is based on the RAMS EN 50126-1 standard (2017), where, in addition to safety and reliability, reachability and sustainability are also addressed.

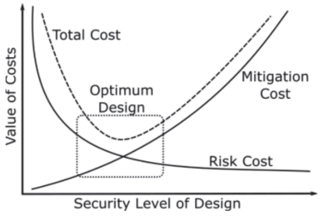

Fig. 2. Cost optimization for safe design.

This sets the situation before the arrival of IEC 62443 (2019). The compilation of the methodology for determining the safety design for the railway as a cyber-physical system can be based directly on the measures from IEC 62443 standard. However, within the railway environment, the technical specification TS 50701 (2021) has been developed, which deals specifically with the interconnection of railway standards with the IEC 62443 standard.

When compiling the methodology for determining the security design for CPS, we proceed from the TS 50701 specification with a possible comparison with the relevant passages of IEC 62443. The working group that compiled TS 50701 also developed several methodological procedures and recommendations of Schlehuber (2021) and Ciancabilla (2021), which are also used in its application.

The methodology is developed within the framework of the rules for handling sensitive company data and thus contains both, the public parts presented to the customer and the corporate know-how that is subject to confidentiality. As part of the communication with the customer, it is important to prove that the resulting safety design was created within the framework of a standardized procedure. The standardized procedure can be broken down into 7 steps: **ZCR1** – Identify the System under Consideration; **ZCR2** – Initial cyber security risk assessment; **ZCR3** – Partition SuC into zones and conduits; **ZCR4** – Risk comparison; **ZCR5** – Detailed cybersecurity risk assessment; **ZCR6** – Document cyber security requirements, assumptions, and constraints; and **ZCR7** – Asset owner approval. This list is from IEC 62443-3-2 (2019). ZCR is an acronym for "Zone and Conduit Requirement". The process model to which the ZCR statement corresponds can be divided into 2 parts. The first part contains ZCR1-ZCR3 and deals with the definition of the system under consideration (SuC), Figure 3.

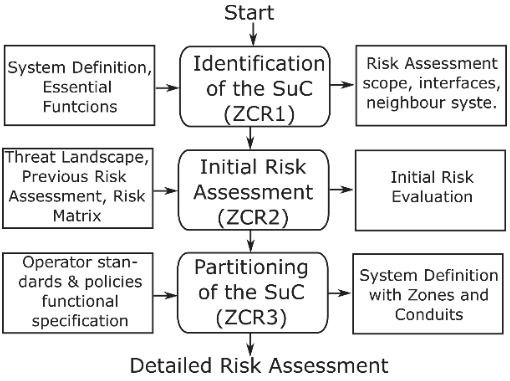
Start
System Definition, Essential Funtcions
Identification of the SuC (ZCR1)
Risk Assessment scope, interfaces, neighbour syste.
Threat Landscape, Previous Risk Assessment, Risk Matrix
Initial Risk Assessment (ZCR2)
Initial Risk Evaluation
Operator standards & policies functional specification
Partitioning of the SuC (ZCR3)
System Definition with Zones and Conduits
Detailed Risk Assessment

Fig. 3. Process model for defining the system under consideration for the purpose of risk identification, IEC 62443-3-2 (2019).

After, they are three more steps, ZCR4-ZCR6, which address a detailed risk analysis, Figure 4. When performing these steps, the application of

IEC 62443 alone is not sufficient. The railway-specific risk management requirements, TS 50701 (2021), should also be considered.

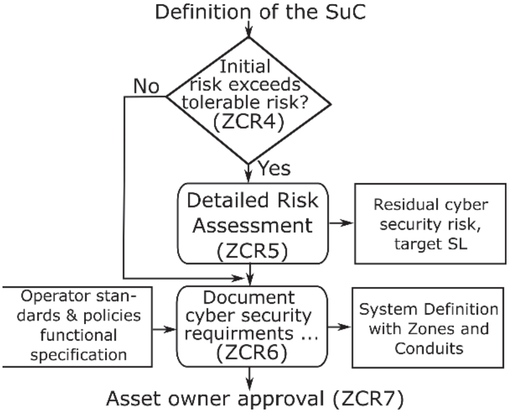
Definition of the SuC
Initial risk exceeds tolerable risk? (ZCR4)
No
Yes
Detailed Risk Assessment (ZCR5)
Residual cyber security risk, target SL
Operator standards & policies functional specification
Document cyber security requirments ... (ZCR6)
System Definition with Zones and Conduits
Asset owner approval (ZCR7)

Fig. 4. Process Model of Risk Identification for Safety Design, IEC 62443-3-2 (2019).

The last step, ZCR7, which is also seen in Figure 4, has a commercial or managerial character in addition to its technical character determined by standards.

5. Procedure for Security |Design Creating

Based on the above-mentioned tools, a methodology for determining cyber-security design on the railway was created. The methodology is based on the standards listed above, but also considers the company's procedures set in risk management and quality management.

The first step is to assemble a team that evaluates the risks and designs the safety design according to the methodology. The team should include at least 3 people from different fields (designer, project manager, quality manager) due to the diversity of views on the solution. In the case of more complex systems or interfaces, the team may be larger.

It is not possible to deal with the whole methodology in detail here, given its scope. Therefore, we will only describe from what parts it becomes. The 7 steps from the previous chapter are reflected in the internal structure of the methodology: 1 - General items; 2 - Distribution of assets; 3 - Defining threats and vulnerabilities; 4 - Risk comparison; 5 - Division of assets into zones and conduits; 6 - Detailed risk assessment; 7 - Defining an SL-vector; 8 - Evaluation of compliance with requirements; 9 - Documentation of cybersecurity requirements, assumptions and limitations; 10 - Approval of the owner of assets; and 11 - Attachments.

Items 1 and 11 serve to correctly apply the methodology. Item 1 specifies the rules and conditions for the use of the method, or the procedure for assembling a team for its application. Item 11 contains some tools that are or can be used in the application of this methodology.

Items 2-6 correspond to the first five ZCR, during which the system under consideration is defined and the risks subsequently identified. Items 9 and 10 correspond to ZCR6 and ZCR7, process documentation and approval of the protected interests by the owner.

There are 2 extra items in the list (items 7 and 8). Item 7 deals with the result of the whole process, which is SL vectors. SL – vector defines which requirements, detailed in IEC 62443 (2019) and to what extent they should be met.

While the other items follow the requirements set in the standards, item 8 is based on the company's risk management practices. Technical standards and specifications assume that the procedures, processes and requirements described therein are flawlessly met. In practice, however, it is necessary to provide control mechanisms that will help to achieve this state. Thus, in item 8, the effectiveness of the security design in item 7 is evaluated in relation to item 3, during which threats and a weak bowl were defined.

During the process of determining the safety design, 39 tables are drawn up in turn. The names of these tables illustrate in more detail what steps are taken during this process:

- **T_1**: Division of individual areas.
- **T_2**: Division of functions into assets.
- **T_3**: Categorize threats.
- **T_4**: Threat severity rating.
- **T_5**: Quantifying the severity of threats.
- **T_6**: Asset Impact Table.
- **T_7**: Quantification of the impact of assets.
- **T_8**: Determination of the acceptable level of risk for the asset.
- **T_9**: Criteria for assessing the level of risk.
- **T_10**: Table of asset allocations into zones and interconnections.

- **T_11**: Zoning and risk-based interconnections.
- **T_12**: List of threats and vulnerabilities versus follow-up.
- **T_13**: Assessment of Assets in terms of type assets.
- **T_14**: Table of calculated partial threats.
- **T_15**: List of individual requirements set by the standard.
- **T_16**: Criteria for determining the severity of the measure.
- **T_17**: Severity matrix (aggregated).
- **T_18**: Pareto analysis.
- **T_19**: Risk Management Plan.
- **T_20**: List of any risk control measures.
- **T_21**: Threats and vulnerabilities versus zones and interconnections.
- **T_22**: Vector/requirement versus zone/link SL table.
- **T_23**: Threats and vulnerabilities versus areas.
- **T_24**: Resulting values for each zone/interconnection.
- **T_25**: Calculation of resulting SL-vectors.
- **T_26**: Assignment of SL_T for individual requirements set out in EN IEC 62443.
- **T_27**: Monitoring the fulfilment of individual target SLs.
- **T_28**: Assessment of Assets in terms of type assets (Confidentiality).
- **T_29**: Assessment of Assets in Terms of Type Assets (Integrity).
- **T_30**: Assessment of Assets in Terms of Type Assets (Availability).
- **T_31**: Assessment of Assets in terms of type assets (Reliability).
- **T_32**: Assessment of Assets in Terms of Type Assets (Security).
- **T_33**: Assessment of Assets in terms of type assets (Maintainability).
- **T_34**: Assessment of Assets in Terms of Type Assets (Vulnerability).
- **T_35**: Assessment of the threat in terms of type assets (Frequency).
- **T_36**: Assessment of the threat in terms of type assets (Impact).
- **T_37**: Assessment of the Threat in terms of type assets (Vulnerability).
- **T_38**: Table of consequences and impacts.
- **T_39**: Probability table.

Listed tables are interconnected in a certain sequence. It is therefore possible to quickly monitor the impact of any changes on subsequent parts of the process. In addition to these tables, which are part of the documentation (ZCR6) of cybersecurity design, there will also be an address table linking standards, documentation, and reports.

From the lists, we can, in terms of importance, point out the "T_10" (ZCR3), which concludes the introductory process of defining the system under consideration from Figure 3. As part of this step, we will divide all protected interests into zones and conduits. Risk analysis and the design of measures are then done in connection with zones and their interfaces. This saves work, where not every protected interest is separately analyzed. However, it is necessary to make an appropriate division according to logical links and security requirements.

The aim of creating a safety design is the "T_26" (ZCR5) from the previous list. An example of "T_26" is in Table 1. Rows in the table correspond to "System requirement" (SR) from IEC 62443 (2019). The columns are prepared:

- Threats according to ENISA (2018).
- Vulnerabilities according to INL/EXT-10-18381 (2010).

Table 1. Example of a table for the final determination of the safety design.

Z1		THREATS						VULNERABILITIES									
(IAC)	***SL***	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
SR 1.01	***1***	▨	▨		▨		🟦		▨	▨		🟦	🟦	▨	▨	🟦	🟦
SR 1.01 RE(1)	***2***	▨	▨		▨		🟦		▨	▨		🟦	🟦	▨	▨	🟦	🟦
SR 1.01 RE(2)	***3***	▨	▨		▨		🟦		▨	▨		🟦	🟦	▨	▨	🟦	🟦
SR 1.02	***2***	▨	▨		▨		🟦		▨	▨		🟦	🟦	▨	▨	🟦	🟦
SR 1.02 RE(1)	***3***	▨	▨		▨		🟦		▨	▨		🟦	🟦	▨	▨	🟦	🟦

Only white columns are filled in. Gray columns are not relevant to the issue, and blue bars do not specify a target security level (SL). The grey and blue columns shall be determined during the application of the methodology described. The resulting SL-vector is given by the highest SL in the rows.

The following tables (T_27-T_39) are then used to check compliance with the requirements set by the safety design and whether the design itself corresponds to the set goal within the chapter of the methodology "8. Evaluation of compliance with requirements (risks)".

6. Conclusion

In the article, we described the circumstances in which we created a methodology for determining cyber-security design. The main motivation is the need to ensure the security of systems and products already at the design stage, because during operation it is more difficult to deal with risks. This new methodology was created under the influence of new challenges in the field of cybersecurity. It has been developed specifically for the railway environment to consider its specifics.

The main sources for the methodology are railway standards – EN 50126-1, TS 50701 cybersecurity – IEC 62443 and ISO 9000 management. The outputs of these standards have been processed into the process of system definition, risk analysis and identification of appropriate measures.

The result was a document that dealt with the technical aspects of the safety design determination process. This document still needed to be supplemented with procedures that consider other aspects of system development proposals. Economic accessibility and difficulty of implementation are some of them. But the most important thing is to set the control mechanism at the end that the proposed design really meets the set goals.

The resulting methodology for determining the safety design is part of the company documentation and is used in practice. However, it is also necessary to modernize the procedures for the implementation and verification of security design, which is part of the subsequent development of methodologies.

This document serves as tool to create security design with cybernetic measures which fulfil railway infrastructure security and safety demands without inconsistences from different are of applications. The methodology was used to compile security design of mobile communication gateway on railway. Two different designs were compiled, one for requisites of project COSMOS (2021) and one for requisites of project ADMORPH (2020).

Acknowledgement

This work is part of the ADMORPH project under grant agreement No. 871259 and COSMOS project under grant agreement No. 957254, funded by the European Union's Horizon 2020 research and innovation programme. It is also part of project CK01000095 under TAČR program DOPRAVA 2020+.

References

ADMORPH. (2020). Towards Adaptively Morphing Embedded Systems. EU, Horizon 2020, no 871259.

Boss, J. (2020). Railway Signalling and Cyber Security. Doctor´ Thesis. Delft: Technical University Delft 2020, 100 p.

Ciancabilla A., Magnanini G., Sperotto F., Amato D. (2021). Application of FprTS 50701, ENISA-ERA Conference: Cybersecurity in Railways.

COSMOS (2021). DevOps for Complex Cyber-physical Systems. ID: 957254, EU H2020.

EN 50126-1. (2017). Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). CENELEC, Brussels.

ENISA (2018). ENISA Threat Landscape Report 2018. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications /enisa-threat-landscape-report-2018

IEC 62443. (2019). Security for Industrial Automation and Control Systems. International Electrotechnical Commission / International Society of Automation. IEC and ISA.

INL/EXT-10-18381 (2010). Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

ISO 9000. (2015). Quality Management Systems. International Organization for Standardization.

ISO/IEC 27001 (2022). *Information Technology — Security Techniques — Information Security Management Systems — Requirements.* ISO.

Lee, E. A. (2008). *Cyber Physical Systems: Design Challenges.* DOI 10.1109/ISORC.2008.25

Movably, P., Kertis, T., Procházková, D., Procházka J. Cyber Security of Metropolitan Railway Communication Infrastructure. In: Risks of

Business and Territorial Processes. ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, pp.78-91.

NIST SP 800-30 (2012). Information Security. *Guide for Conducting Risk Assessments.* NIST.

Procházka, J., Hošková-Mayerová, Š., Procházková D. (2019). The risks connected with accidents on highways and railways. ISSN 0033-5177, e-ISSN 1573-7845. Springer Netherlands.

Procházka, J., Procházková, D. (2022). Risk Management of Railway Transport Systems. Praha: CVUT, doi:10.14311/BK.9788001069950

Procházková, D. (2017). *Principles of Risk Management of Complex Technological Facilities.* Praha: ČVUT. Doi: 10.14311/BK.9788001061 824

Schlehuber Ch, Benoliel C. S. (2021). CENELEC prTS 50701 (Railway Applications – Cyber Security). ENISA-ERA Conference: Cybersecurity in Railways.

Schneier, B. (2002). . *Schneier on Security.* New York: John Wiley & Sons 2002.

TS 50701 (2021). Railway Applications – Cybersecurity, draft version D8E5, CENELEC.

ZAIRI, M. (1991). Total Quality Management for Engineers. Cambridge. Woodhead Publishing Ltd.