# Cybersecurity Standards of Intellectual Transport Systems

**Alexey Ozerov**

*Research and Design Institute for Information Technology, Signalling and Telecommunications on Railway Transport (NIIAS, Moscow, Russia, a.ozerov@vniias.ru*

**Contribution to the State of the Art**

https://doi.org/10.7251/JIT2302104O UDC: 004.056.5:656.222

**Abstract**: The paper gives an overview of general approaches and existing standards as regards the cybersecurity of automated control systems with the railway transport specifics taken into account. It outlines major directions for the development of guidelines and activities for ensuring the cybersecurity of intellectual control systems.

**Keywords:** safety/security, functional safety, cybersecurity, risk assessment, system lifecycle, cyber ranges.

The modern railway control/management systems are characterised by a high level of integration and connectivity. On the one hand, that is due to a wide use of computer technology, single data communication buses, digital diagnostics sensors, etc. On the other hand, that is also a basic prerequisite for further development and widespread deployment of intelligent transportation systems.

Given the major trend towards cloud technology, further adoption of intelligent control/management systems in railway transportation means a constantly growing attack surface (primarily, for cyberattacks). Due to that fact, it is required to reconsider the attitude to ensuring cybersecurity of control/management systems not only at the stage of operation, but at the design stage as well. Of increasing importance are industry-specific recommendations, guidelines, and standards that examine the principles of designing secure control/management systems holistically while taking into account the principles of functional safety and the possible mechanisms of ensuring cybersecurity as part of a single balanced approach.

Meanwhile, working out an all-purpose approach in this area is not at all a trivial task. The lifecycle of railway signalling systems is anywhere from 15 to 30 or 50 years, while the functional safety principles of such systems remain unchanged since the era of relay technology. Meanwhile, the cyber integration of modern systems is moving forward and the cyber threat landscape is constantly changing requiring prompt reaction and improvement of defence mechanisms.

The experts do not have a single interpretation of the concepts of “information security” and “cybersecurity” as regards information management systems and their logical association. Thus, some experts believe that information security is a component of cybersecurity, while others insist on the opposite, claiming that cybersecurity is part of information security. That causes the differences in the approaches to ensuring cybersecurity of control/management systems. In one case, they insist on developing special methods of protection aimed at eliminating wrong-side failures, while in others, they claim that the conventional information security methods suffice and do not require taking into account the specificity of railway control/management systems [1].

Additionally, we must also point out the difference in the interpretation of the above concepts as regards non-safety-related systems (generally referred to as information communication technologies, ICT) and critical systems (the so-called supervisory control and data acquisition, SCADA). If, in the case of ICT, the classic "confidentiality – integrity – availability" triad is shifted towards confidentiality, in the case of SCADA, it is shifted towards availability (see Fig. 1) [2].

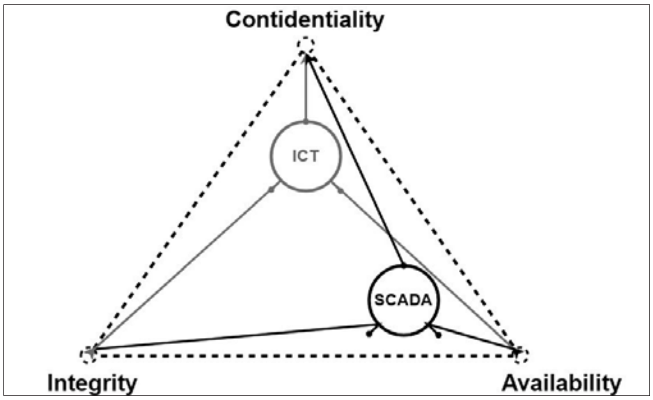

*Fig. 1. Information/cybersecurity triad*

Unlike in the case of ICT, the primary SCADA cybersecurity threats are wrong-side failures that may be caused by both cyberattacks and exploitation of undocumented features in a system's software and components. Naturally, they can also be caused by hardware and software failures and faults in the system's operation, operator errors, and input of erroneous data [3].

As it is known, the designers of vital railway systems conventionally follow the "safety above all" paradigm, meaning that each system component (and the entire system) are to comply with a certain Safety Integrity Level (SIL). In order to achieve the required SIL, certain design rules and test methods are to be implemented that guarantee that the system will continue fulfilling the appropriate safety requirements in the case of a random failure. However, functional safety standards that are used as guidelines for railway system design do not take matters of cybersecurity into consideration, but merely mention that a cybersecurity mechanism is to be developed in accordance with the recommendations of the standards that deal with general-purpose network device security. The primary standard IEC 61508 [4] that describes the requirements for the functional safety of electrical and electronic devices and the CENELEC EN 50159 [5] standard that describes the requirements for data communication within critical railway systems only mention that the possibility of intentional actions of people is to be taken into consideration and refer to the ISA/IEC 62443 [6] standard.

Due to that various international organisations are developing recommendations and guidelines that attempt consolidating functional safety requirements for railway signalling systems and cybersecurity requirements. Thus, in 2015, the International Union of Railways (UIC) initiated the ARGUS project that brought forth guidelines for the cybersecurity of railway systems [7] that extrapolate the risk evaluation principles and assurance of information security of the ISO/IEC 27000 series of standards to the railway signalling and communication systems. The Guidelines for Cyber Security in Railway has actually become the first international document developed with extensive participation of experts in not only information security, but railway signalling as well.

Several projects of the Shift2Rail European initiative also attempted a comprehensive consideration of the matters of cybersecurity of railway control/management systems. Out of those, the following should be noted:

- the 4SECURail project that developed formal methods for ensuring security in a railway environment and recommended creating "computer security incident response teams" (CSIRT) for the railways [8];
- the CYRail project that published various guidelines for improving the security of railway systems, including recommendations for designing cyber-attack resilient systems (secure by design) [9].

Of note is the OCORA initiative (Open CCS Onboard Reference Architecture) that has developed guidelines for a cyber-secure reference onboard train control and protection systems architecture that is largely based on the CYRail recommendations (thorough evaluation of threats and risks, threat model construction, system partitioning, embedded cyber security and monitoring mechanisms) [10].

Of special interest is the EU-funded CLUG project that is dedicated to a more specific task, i.e., the development of a secure onboard train control and protection unit architecture featuring a GNSS-based positioning system taking into account cybersecurity among other things. The project participants are developing requirements for the onboard unit based on the risk evaluation method and the four safety categories according to ISA/IEC 62443. The following threats are taken into consideration: data diddling, spoofing, distortion of measured data supplied by sensors, damage to digital track map databases, output data falsification, denial of service [11].

The existence of a wide class of threats and the variety of ways of dealing with them – in terms of the principles of ensuring functional safety, physical protection of devices and information security – indicates not only the absence of a specialised railway standard, but the complexity of the matter. The authors of [12] conclude that the conventional approach, whereas the matters of cybersecurity are considered only as an addition to functional safety and solved only through methods of information protection, is to be abandoned. An integrated approach is required that would involve the development of the system's digital infrastructure with built-in cybersecurity mechanisms.

Probably, when it has become a new standard, the CENELEC prTS 50701 Railway applications – Cybersecurity technical specification will contribute to the development of an integrated approach [13]. This pre-standard is based on the ISA/IEC 62443 standard and is a specialised solution for the railway industry, including rolling stock, signalling and infrastructure.

The key provision of the prTS 50701 draft standard is the principle of in-depth defence built upon a multi-level security system. PrTS 50701 defines a concept of security levels that largely resembles the approach based on the safety integrity levels (SIL), yet differs from it in several details. In particular, it states that the security level is the measure of confidence that a zone of the system architecture, conduit, communication channel or a component thereof is free from vulnerabilities and functions as intended. PrTS 50701 defines architectural design constraints for railway technology based on the concept of zoning. PrTS 50701 specifies that zoning involves measures for functionality encapsulation for the purpose of keeping a particular service alive in case of an incident in another zone while isolating it by closing the gateways to the affected zone.

According to [14], the basic ISA/IEC 62443 standard is the optimal industry standard in cybersecurity, and in combination with prTS 50701 provides all the required guidelines for ensuring cybersecurity of railway systems.

Nonetheless, given the growing relevance of cybersecurity in the context of modern control/management systems, not only the conventional SIL-based design approach, but the entire lifecycle concept of critical railway control/management systems that is usually depicted with the V model must be reconsidered. The initial cybersecurity risk assessment of a system under development is to be

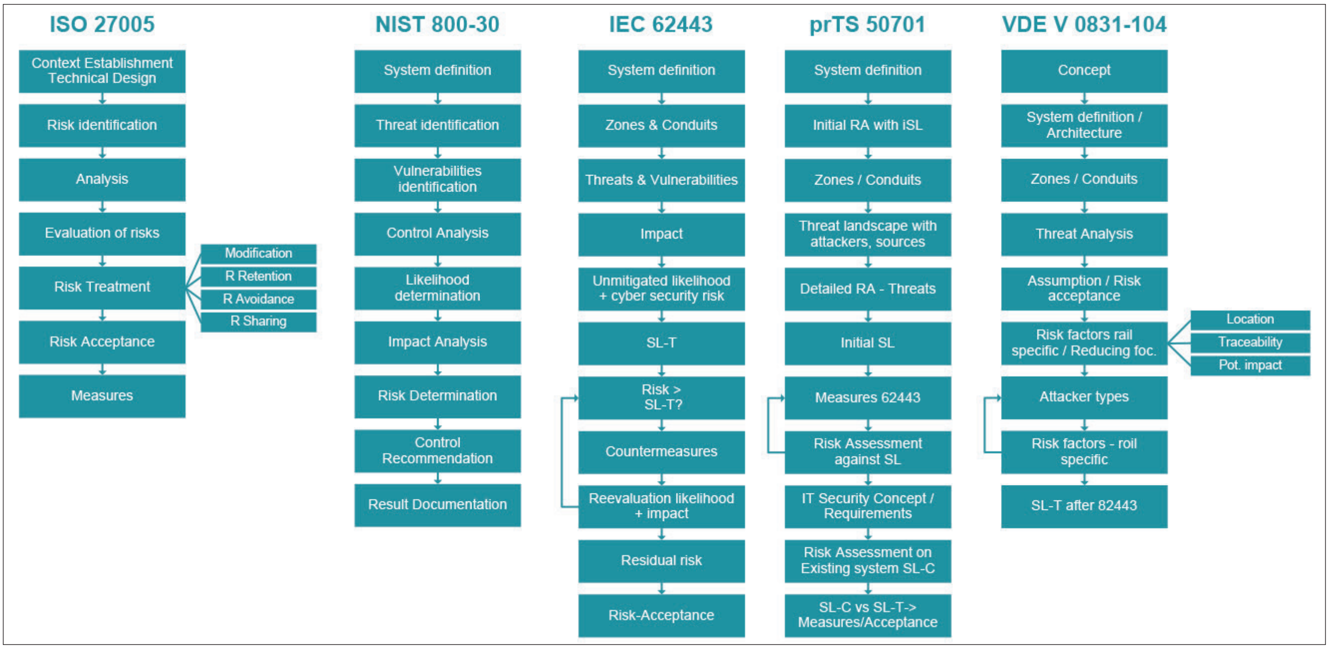

***Fig. 2.*** *Risk evaluation models at system development stages defined in standards*

conducted at the very early stage of concept and requirement definition. Fig. 2 shows the approaches of various standards to the evaluation of risks at various stages of vital control/management system design.

Selecting the most optimal system development process requires conducting the appropriate evaluation procedure. The key evaluation criteria are as follows:

- compliance with the operation processes employed in railway transportation;
- compliance with industry standards and requirements of the certification and regulatory agencies;
- usability;
- efficiency;
- level of detail defined by the standard;
- lack of excessive complexity.

According to IEC 62443 and prTS 50701 the process of risk evaluation is to include the following stages:

1) description of the examined system;

2) pre-zoning principle based on preliminary risk evaluation;

3) definition of basic threat types;

4) assessment of motivation, knowledge, and resources of attackers;

5) definition of specific types of threats, including those on the railway company's register;

6) classification of threats according to the basic requirements;

7) definition of the initial level of security for each threat in accordance with the basic requirements;

8) input of preliminary value zones defined in the basic documents into data vectors;

9) calculation of the security levels for preliminary zones after the definition of the maximum vector values;

10) definition of final security levels using correction coefficients (maximum value 1);

11) performance of cybersecurity measures;

12) verification of whether the measures are applicable to the concept of preliminary zoning, provided that they comply with the respective requirements. If the measures are not applicable, the concept is to be reconsidered;

13) the performance of items 11 and 12 is to be repeated until all system settings have been performed.

All of the stages of the cybersecurity solution development processes are to be coordinated with the respective system lifecycle stages performed based on the requirements of CENELEC standards. That enables verification and validation, especially as regards obtaining representative results that can be conveniently used as output data in the course of the process. Fig. 3 shows an example of the V model of a railway signalling system's lifecycle that integrates cybersecurity measures that was developed

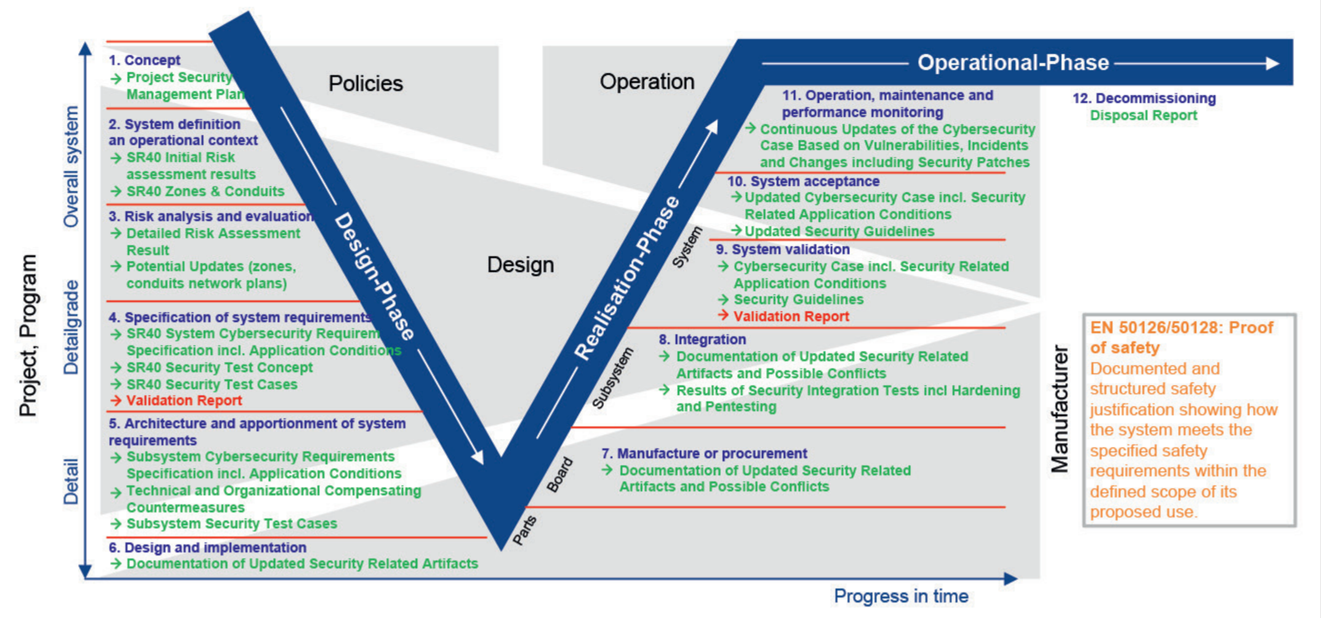
Project, Program
Overall system
Detailgrade
Detail
1. Concept
→ Project Security Management Plan
2. System definition an operational context
→ SR40 Initial Risk assessment results
→ SR40 Zones & Conduits
3. Risk analysis and evaluation
→ Detailed Risk Assessment Result
→ Potential Updates (zones, conduits network plans)
4. Specification of system requirements
→ SR40 System Cybersecurity Requirem Specification incl. Application Conditions
→ SR40 Security Test Concept
→ SR40 Security Test Cases
→ Validation Report
5. Architecture and apportionment of system requirements
→ Subsystem Cybersecurity Requirements Specification incl. Application Conditions
→ Technical and Organizational Compensating Countermeasures
→ Subsystem Security Test Cases
6. Design and implementation
→ Documentation of Updated Security Related Artifacts
Policies
Design-Phase
Design
Operation
Parts
Board
Subsystem
System
Realisation-Phase
Operational-Phase
7. Manufacture or procurement
→ Documentation of Updated Security Related Artifacts and Possible Conflicts
8. Integration
→ Documentation of Updated Security Related Artifacts and Possible Conflicts
→ Results of Security Integration Tests incl Hardening and Pentesting
9. System validation
→ Cybersecurity Case incl. Security Related Application Conditions
→ Security Guidelines
→ Validation Report
10. System acceptance
→ Updated Cybersecurity Case incl. Security Related Application Conditions
→ Updated Security Guidelines
11. Operation, maintenance and performance monitoring
→ Continuous Updates of the Cybersecurity Case Based on Vulnerabilities, Incidents and Changes including Security Patches
12. Decommissioning
Disposal Report
Manufacturer
EN 50126/50128: Proof of safety
Documented and structured safety justification showing how the system meets the specified safety requirements within the defined scope of its proposed use.
Progress in time

***Fig. 3.*** *An example of the V model that shows the correlation between the CENELEC standard requirements and assurance of cybersecurity*

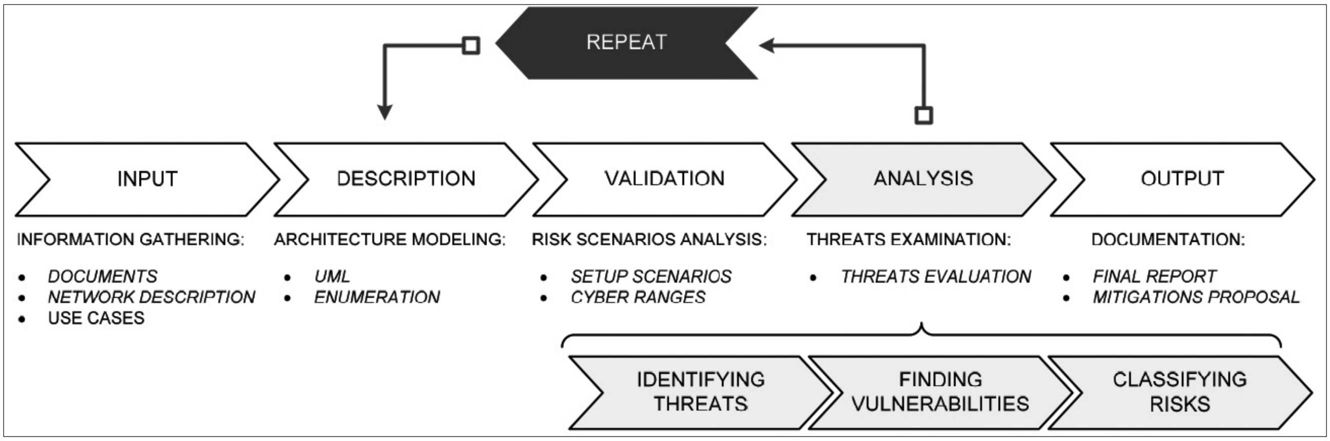

***Fig. 4.*** *Control/management system cybersecurity risk evaluation process*

as part of the Smartrail 4.0 railway innovation program of Switzerland.

Thus, cybersecurity risks are to be evaluated at all system lifecycle stages, and at the stage of verification and validation is to become an integral part of integrated safety assessment that includes the assessment of its cyber resilience subject to the constructed model of cyber threats. The overall risk evaluation process according to those standards is shown in Fig. 4 where the primary analysis procedure and its main stages are shown in grey.

We must note the ever growing popularity of the idea of cyber ranges that involves conducting the required tests within certain virtual boundaries and ensures isolation from operational devices. Cyber ranges enable the performance of tests required by the safety analysis through a rapid simulation of the required scenarios. For instance, the European CONCORDIA consortium is actively working on creating cyber ranges [15].

Cyber ranges may be physical or completely virtual, whereas cyber range scenario components use a virtualisation solution for the purpose of emulating physical assets, as well as hybrid, whereas solutions are employed that are based on a combination of hardware, virtualised, and simulated elements. As the process of virtual scenario definition is quite demanding, it is obvious that most efforts are to be concentrated in its automation with the use of various software solutions. A most important tool for virtual scenario definition is gamification that has been used for a long time in simulation and cyber security risk evaluation.

Today, one of the most pressing problems is the integration of the existing tools for testing system security into digital twins. Another unsolved problem is meeting the computational requirements of the precision simulation environments. Indeed, if the final goal consists in emulating an intelligent control/management system in its entirety, it is obvious that the required computational resources may prove to be above the current technical capabilities. A wide use of artificial intelligence as part of cyber security risk evaluation using cyber ranges can also be restricted by limited computing capabilities.

## References

[1] Ozerov A.V. Cybersecurity of Railway Command and Control Systems. Journal of Information Technology and Applications 2019;9(2):53-59. DOI 10.7251/JIT1902053O.

[2] Soderi S., Masti D., Lun Yu.Z. Railway cyber-security in the era of interconnected systems: a survey. IEEE; 2022. (accessed 14.03.2023). Available at: https://arxiv.org/pdf/2207.13412.pdf.

[3] Shubinsky I.B., Makarov B.A. [A little about cyber security]. Information, Communications, Informatics 2014;8:15-18. (in Russ.)

[4] IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Switzerland: IEC; 2010.

[5] CENELEC EN 50126:2018. Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Belgium: CENELEC; 2018.

[6] ISA/IEC 62443:2009. Security for Industrial Automation and Control Systems. USA: ISA; 2009.

[7] Guidelines for Cyber Security in Railway. France: UIC; 2018.

[8] 4SecuRail. EU; 2023. (accessed 07.03.2023). Available at: https://www.4securail.eu/.

[9] CYRail. EU; 2023. (accessed 14.03.2023). Available at: https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf.

[10] OCORA-TWS06-020, Version: 1.00. EU: RCA; 2021.

[11] The Clug Project. EU; 2023. (accessed 10.03.2023). Available at: http://www.clugproject.eu/en/news/establishing-security-requirements-gnss-based-train-localisation-

board-unit-tlobu.

[12] CENELEC CLC/TS 50701:2021. Railway applications – Cybersecurity. Technical Specification. Belgium: CENELEC; 2021.

[13] Bearfield G., Van Gulijk C., Parkinson S., Thomas R.J. Transformation of Cyber Security/Safety Assurance. World Congress on Railway Research; 2022.

[14] Parkinson H.J., Basher D.R., Bamford G. Railway cyber security and TS50701. 2022. (accessed 10.03.2023). Available at: https://www.researchgate.net/publication/361006662_Railway_cyber_security_and_TS507.

[15] CONCORDIA. EU; 2023. (accessed 09.03.2023). Available at: https://www.concordia-h2020.eu/news/concordia-releases-an-open-source-cyber-range-platform/.

Received: September 29, 2023
Accepted: November 13, 2023

## About the authors

**Alexey Ozerov** is the Head of International Department – Head of Intellectual Property Management Centre of JSC NIIAS. He has been working with JSC NIIAS for over 16 years in various positions related to research, signalling business unit and international cooperation. He is finishing his PhD in traffic management and has authored over 50 papers and 8 patents in the field of advanced railway signalling and traffic management.

**For citation**

Alexey Ozerov, Cybersecurity Standards of Intellectual Transport Systems, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 13(2023) 2:104-109, (UDC: 004.056.5:656.222), (DOI: 10.7251/JIT2302104O, Volume 13, Number 2, Banja Luka, December (57-120), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004