Railway Infrastructure Cybersecurity: An Overview

João Nunes, Tiago Cruz and Paulo Simões
University of Coimbra, CISUC, DEI, Portugal

jpbn@student.dei.uc.pt
tjcruz@dei.uc.pt
psimoes@dei.uc.pt

Abstract: The railway infrastructure constitutes a type of operational technology (OT)-based critical infrastructure, which is expected to work 24x7, 365 days a year, and where the life expectancy of operational equipment often exceeds 30 years. In this domain, an operational anomaly compromising the OT system can cause a train accident or interrupt traffic, with potentially significant impact in terms of business as well as for passenger safety. Due to their relevance, railways are strategic assets of national interest and, consequently, targets of interest for cybercriminals and cyberwarfare activities. For instance, service interruptions may trigger ripple effects resulting in product shortages and widespread supply chain disruptions, with severe impacts for both the economy and national security. In a bid to optimise and streamline operations. the railway industry has recently started taking a series of significant steps towards digitization, with infrastructures experiencing a significant paradigm shift which, for instance, makes it possible to have centralised interlockings and Radio Block Centre (RBC) for an entire country, with geographical redundancy, ensuring the utmost availability and punctuality by moving the control logic to the cloud. Nevertheless, these developments must always be carried on within the scope of established cybersecurity standards and frameworks. This paper presents an analysis of the state of the art on railway cybersecurity, focused on the existing solutions based on the application of the CENELEC "Technical specification 50701 - Railway Application – Cybersecurity", which is currently the latest European specification addressing railways, being designed to help suppliers, integrators, and operators to implement a cybersecurity risk assessment plan, the necessary controls, and the management of the complete system life cycle. Special attention will be paid to the conduit between the rail signal interlocking system, that controls the line signalling, and the Automatic Train Supervision (ATS) that runs in the Operational Control Centre (OCC), as this has been identified by the European Union Agency for Cybersecurity (ENISA) as one of the most critical systems identified by the operators of essential services.

Keywords: Railways, OT Security, Cyber-Physical Systems, Cybersecurity, Critical Infrastructure Security

1. Introduction

As today's world gets more interconnected, with every system getting more technologically complex, the railway industry is also evolving. With the interdependence of systems, railway infrastructures – that, until a few years ago, were considered safe, since they were not connected to the exterior – are now regarded as potential targets for cyber attacks, due to their economic and societal relevance. As a result of this new cyber landscape, agencies, integrators, and operators face the need to develop cybersecurity standards, specifications and guidelines specifically applied to the railway ecosystem.

Typically, a railway infrastructure is made of several (sub)systems. Among those, according to (Malatras, 2023), the most critical ones are the Interlocking system (IxL) and the Control Centre or Automatic train supervision (ATS). The IxL controls all the signalling and track moving parts, for instance avoiding that multiple trains simultaneously use the same track segment. On the other hand, the ATS is where the train routing and traffic management decisions are taken, and where all train movement is logged. Nowadays, both systems rely on a high level of automation, which also happens to the majority of the other railway subsystems, such as passenger announcing systems, power line control systems and train to track systems. A high-level view of the functional structure of the rail traffic management system is presented in Figure 1.

Overall, the coordination of all those subsystems leads to quite complex railway ecosystems, which poses significant challenges from a cybersecurity point of view. To cope with this situation, in 2021 CENELEC introduced the CLC/TS 50701:2021 (CENELEC, 2021), later updated in 2023 (CENELEC, 2023) and often considered as the world's first international standard to offer comprehensive cybersecurity guidance tailored specifically for rail applications. Nevertheless, the effective adoption of this standard will be a slow and difficult process, due to its complexity, the slow adoption timescale of railway systems, and the need to keep supporting legacy components for a long time.

In this paper we contribute to this ongoing effort by discussing the cybersecurity landscape associated with this recently introduced standard. This contribution is relevant to the cybersecurity community working in the railways field due to the current lack of adequate surveys covering this new standard, which is expected to have a strong impact in this industry.

The rest of the paper is organised as follows: Section 2 provides a general overview of the security of railway systems. Section 3 introduces the reader to the CENELEC TS50701 standard, including the identification of the typical life cycle of railways cybersecurity and the relation with other relevant standards. Section 4 introduces the concepts of interlocking and ATS conduits, also discussing related cybersecurity vulnerabilities and potential countermeasures. Finally, Section 5 concludes the paper.

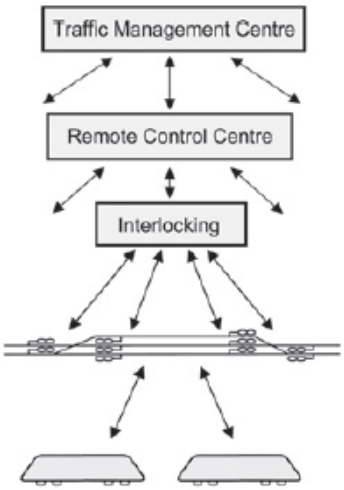

Figure 1: Functional structure (Winter, 2009)

2. Security of Railway Systems

The railway industry is currently undertaking a big step towards digitalization. Moreover, across Europe there is also an ongoing interest towards standardisation and harmonisation, to facilitate cross border service. However, this is an industry where the life expectancy of operational equipment is sometimes over 30 years, which significantly slows down this harmonisation, in terms of technology and security controls. This creates a paradoxical scenario. On one hand, with the rise of the cloud computing paradigm (Cardoso and Simões, 2011), it is possible to have a state-of-the-art system with most of the processing functions and control logic for an entire country being hosted in the cloud (Siemens, 2022). On the other hand, there are still legacy systems running equipment with more or less proprietary technologies from the late 1980s.

Railway infrastructure is a critical Operational Technology (OT) system that is expected to work 24x7, 365 days a year. If something doesn't work as planned, and the OT system is compromised, it can cause train delays, traffic disruption, or even accidents involving dangerous cargo or the loss of human lifes. The potential impact is considerable, both from an economic point of view and from a safety perspective and is prone to induce considerable cascade effects in other critical infrastructures, for instance disrupting supply chain logistics (U.S. Department of Homeland Security, 2022). This turns railways into an attractive target for cyberwarfare.

Moreover, railway systems are potentially more vulnerable to cyberattacks, when compared to IT systems. OT systems such as railways are usually more vulnerable, partially due to a lack of cybersecurity awareness of OT personnel. Because these infrastructures were not originally designed with cybersecurity in mind (long life cycles of 30 years, widespread presence of legacy systems), and because they are less controlled, as well as, spread across a larger geographical area. A railway main line system can have several hundreds of kilometres. For example, the Japanese bullet train, Shinkansen, spreads across 515km, involving a great number of different devices with a great diversity of supply chain (Kapoor, 2022). Security incidents in this type of system can also bring a great impact in the public opinion, due to the great number of people affected. For example, a mass-transit railway system such as the London Tube handles up to five million passenger journeys per day, serving 272 stations (Mayor of London, 2022).

Bearing in mind the criticality, the threats, the vulnerabilities, and the lack of consistency across countries that these OT systems face, the European Union railway suppliers, and operators through the European Committee for Electrotechnical Standardization, recently produced the technical specification CENELEC TS 50701 (Railway applications – CyberSecurity). In the next Section we discuss this technical specification in more detail.

3. Overview of CENELEC TS50701

The CENELEC TS50701 technical specification is directly based on the IEC/EN IEC 62443 series (International Electrotechnical Commission, 2013), which in turn are also related to EN ISO/IEC 27001 (International Organization for Standardization, 2013) and EN ISO 27002 (International Organization for Standardization, 2022). Its goal is to provide a narrower definition and more consistent and specialised approach to the security of a railway system. Previously, system suppliers and railway operators had to resort to more generic standards such as EC/EN IEC 62443 (which has become a horizontal standard as of 2021), which in many aspects missed the specific needs of the railways domain, but are nonetheless relevant.

CENELEC's TS50701 is geared towards railway cybersecurity, aiming at protecting essential system functions. While compliance with this specification may fulfil a specific targeted security level, by adopting state of the art cybersecurity practices, there are factors that can potentially hamper this effort, namely time and budgetary restrictions. Ultimately, cybersecurity becomes a risk management effort focused on achieving a trade-off between effort, budget, and risk tolerance.

3.1 The Life Cycle of Railways Cybersecurity

This technical specification considers thirteen different phases for security-related activities within a railway application life cycle, which directly derive from the standard EN 50126-1 (CENELEC, 2017). More specifically, the following phases are considered:

1. Prerequisites – when the Railway operator's security program is established, and applicable legal and regulatory frameworks are identified.
2. Concept – where the System under consideration (SuC) is identified, along with security-related controls, a High-Level zone model, applicable security standards, and – one of the key points of the technical specification – the definition of purpose and scope. At this stage there must be an alignment between railway operators/asset owners and stakeholder's security goals. The outcome of this phase is the project's cybersecurity management plan.
3. System definition and operational context – corresponding to the definition of system boundaries, and a review of logical and physical network plans, defining the zones and conduits of the network.
4. Risk analysis and evaluation – corresponding to a risk assessment to identify possible threats, along with physical and organisational countermeasures or assumptions for zones and conduits. It should also consider the business continuity aspects (including incident response and recovery) for the system under consideration.
5. Specification of system requirements – in this phase, the SuC-specific refinement of normative requirements should be performed.
6. Architecture and apportionment of system requirements – at this stage the risk assessment if needed should be updated, it should be considered the security-related application conditions, which are explained in Table 6 of (CENELEC, 2021), where an extensive table of security requirements is presented, and its application to the railway environment.
7. Design and implementation – With all the necessary information, now it is time to conclude the design of the solution, it should be prevented and avoided the conflicts between the component cyber security functionality and functional architecture.
8. Manufacture or Procurement – all the necessary material and services are acquired at this phase.
9. Integration – in this phase the network plans should be reviewed considering the new acquired equipment, and it should be made an inventory of all systems and applications. It is also now that the Qualification of security components and functions from test integration results, penetration testing, and vulnerability scanning should be made.
10. System Validation – at this phase it should be Assessed by examination and provision of objective evidence that the SuC in combination with its security-related application conditions complies with the Cybersecurity Requirements Specification, the output of this phase is the Updated System Integrator cybersecurity case.
11. System acceptance – finally we reach the system acceptance, now occurs the security handover between System Integrator and railway operator.
12. Operation, maintenance, and performance monitoring – this is the longest phase in the life cycle of the SuC, across it, is required to perform the maintenance of the logical and physical network plan, as well

as the list of IT systems and installed applications. Perform patch and/or configuration management, data backup and auditing procedures to enable data recovery.

13. Decommissioning – Finally the decommissioning phase, the disposal of components, taking security criteria into account, ensuring that all confidential data and information should be completely erased, and erasure verified during system decommissioning and disposal.

3.2 Other Cyber Security Standards and Guidelines

As presented in (Parkinson et al., 2023), besides the TS50701, there are other standards, and guidelines that could also be applied for the Railway environment, as it is shown in Table 1. Among the referred guidelines, only TS50701 provides some guidance on how cyber security could be managed in the scope of the EN 50126-1 (CENELEC, 2017) Reliability, Availability, Maintainability & Safety (RAMS)-life cycles. The target goal of TS 50701 is to be compatible and consistent with EN 50126-1, when applied to the System under Consideration, as well as to separate the safety approval and cyber security acceptance as much as possible due to their inherent differences in terms of lifecycle (Castanier et al., 2021). TS50701 is the only standard that shows in detail how to implement the complete cyber plan, from prerequisites to decommissioning, and what should be done on each life cycle phase. TS50701 also encompasses a series of technological and organisational countermeasures capable of providing a basic level of assurance for legacy infrastructures conceived without security in mind and which cannot achieve a security level according to IEC 62443 (CENELEC, 2021).

Table 1: Comparisons of Cybersecurity Standards and Guidance (Parkinson et al., 2023)

Standards / Guidance Reference	Main Scope	Links to the EN50126 lifecycle?	Focused on railways?	International Focus?
ISO27001 (International Organization for Standardization, 2013)	IT			Yes
NIST Cybersecurity Framework (Barrett, 2018)	OT & IT			
NIST SP800-82 (Stouffer, 2023)	OT			
NIS Regulations (UK Government, 2018)	OT & IT			Yes
Cyber Essentials (UK Government, 2023)	IT			
AS 7770 (Rail Industry Safety and Standards Board, 2018)	OT & IT		Yes	
IEC 62443 (International Electrotechnical Commission, 2013)	OT			Yes
DIN VDE V 0831-104 (DIN, 2015)	OT		Yes	
TS50701 (CENELEC, 2023)	OT	Yes	Yes	Yes
CYRail D7.5 (CYRail, 2018)	OT		Yes	Yes

IT=Information Technology; OT=Operational Technology

4. Interlocking and ATS Conduit

TS 50701 defines a *conduit* as a logical grouping of communication channels that connect two or more zones, and share common security requirements. In principle, only three different types of conduits are necessary to connect zones, depending on the Security Level of the zones:

- Conduits implementing a transparent gateway (connecting zones with the same security level).
- Filtering conduits as firewall appliances (allowing a zone of lower or equal security level to communicate with a zone of a higher security level).
- And unidirectional conduits, as data diodes (Freitas et al., 2019) or network taps, allowing output from a higher security level zone to others.

The conduit that connects the IxL systems to the ATS is of utmost critical relevance. The IxL systems are responsible for controlling the train exclusive access to a route, which is a sequence of track elements exclusively assigned for train movement through a station or a junction (Soderi et al., 2023). The ATS, or Operations Control Centre, often acts upon the signals generated by the IxL system to monitor and adjust the performance of individual trains, to ensure smooth railway service. It is where the railway operators take decisions and control the railway traffic (Soderi et al., 2023).

4.1 Interlocking Main Vulnerabilities

Concerning interlocking system vulnerabilities, railway infrastructures are distributed over wide geographical areas, where critical nodes of railway systems and networks require maximum availability, and where physical protection and maintenance cost time and money (Liveri et al., 2020). Track side equipment updates can have an important financial repercussion, due to the number of systems and their cost (Liveri et al., 2020). Updating the legacy or obsolete systems (with life cycles calculated in decades) to implement cybersecurity measures is often difficult or even impossible.

4.2 Main Vulnerabilities of Automatic Train Supervision Systems

One of the key vulnerabilities of ATS systems is the lack of consensus on how to conceive such control centres, since many different Operations Control Centre (OCC) configurations have been proposed over the years, often based on non-compatible standards (Soderi et al., 2023). This is aggravated by the generalised adoption of bad practices such as postponing operating system updates and patches indefinitely or provisioning and configuring network equipment with no protective measures enabled – for instance incorrect or non-existent network segregation, using both to provide passenger access and to communicate telemetry data with track-side devices (Gordeychik, 2019). Railway operators also report problems related with low cybersecurity awareness and differences in culture, especially among safety and operations personnel (Liveri et al., 2020). Railway Supervision application developers also suffer from weak cybersecurity awareness, focusing mostly on developing the functionality of the applications and not on their resilience to cyber-attacks, often disregarding good development and lifecycle management practices such as the ones proposed by IEC 62443-4-1 (IEC, 2018).

4.3 Measures to Control Risks at the Conduit Level

4.3.1 Modelling Tools for Cyber-Physical Systems

A few tools and measures have been proposed in the literature to decrease the vulnerability of conduits, as discussed next.

For instance, (Thomas et al., n.d.) proposes a modelling framework for an automated analysis of threats. More specifically, it proposes a tool for evaluating vulnerability based on the CVSS score. It has an interesting way of describing the system under consideration, using the Visio tool as a graphical input. Then, it creates a mathematical model of the system as a directed graph, including the data flows between the components. It is also necessary to define which assets could be vulnerable to an attack. Finally, in the last step, the attacker is characterised. The framework allows to determine attack vectors and possible attack paths, based on statistical analysis. It also provides a cost-effective way of testing possible attack scenarios. The framework also allows estimating the impact of an attack, based on which nodes have been compromised. This makes it possible to understand how attacks propagate, often pinpointing less obvious and neglected propagation paths. Finally, the framework also makes it possible to quickly test new strategies of mitigation.

Another interesting study is presented in (Adamos et al., 2024), which recommends segregating the OT and IT networks from the beginning. This recommendation is motivated by two main reasons: first, the type of traffic conveyed for each domain is totally different, often presenting distinct (and possibly competing) requirements. Second, the interconnection of OT and IT traffic introduces extra attack vectors. Thus, segregation can be based on a defence in depth approach, focusing on the critical functions of the conduit.

Additionally, there might be constraints – for instance, in IEC 61850 scenarios a mandatory response time of less than 4ms advises against the use of network encryption (Gaspar et al. 2023). As a result, a comprehensive risk assessment is required, to adapt the security measures to the operational requirements or to choose the tools and technologies whose performance better suit the specific scenario needs (Rosa et al., 2015). To better understand the risk of the conduit or the system, in (Adamos et al., 2024) they have developed a tool called

CPSRA (cyber physical risk assessment), based as well in graph theory, according with the authors, it performs automatic complexity analysis of the Cyber-physical systems (CPS), and its goal is to improve the resilience of the system. When creating the model of the real-world system, it considers the CVE vulnerabilities of each component and produces an isomorphic graph of the test model. The output of the tool identifies the high-risk components and potential sub-attack and subliminal attack paths. It also suggests mitigation points for the implementation of security controls. The tool also gives a new perspective to the security team, where sometimes a component may not include a high -impact CVE, could be a critical component due to its location in the overall architecture. As well as the tool previously described, this one allows to perform an automated risk analysis, saving time, where normally this task would be done manually.

4.3.2 Methodology

The authors of (Prochazka et al., 2023) propose a deeper and more practical approach to the security design part of the project, when compared with the standard approach prescribed in IEC 62443-3 and, consequently, in TS50701. The motivation for this methodology is the need to ensure the security of systems and products at the design stage – since when the project is already in the field it becomes much more difficult and costly to perform any changes. As it also considers a more enterprise-focused perspective, it should also include the company's risk management practices. In the proposed methodology, the process of determining the safety design (corresponding to phases 1 to 6 of TS50701) is replaced in detail by a total of 39 tables: 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.

As the listed tables are interconnected, it becomes possible to perform changes on one of the tables and monitor the cascade impact on interrelated tables. This approach has already been used in two different projects to compile the security design of mobile communication gateways on railways.

4.3.3 Virtual Test Platforms

Virtual test platforms are an important complement to the modelling tools previously described from (Thomas et al., n.d.) and from (Adamos et al., 2024), as well as to the detailed approach proposed by (Prochazka et al., 2023).

As described in (Soderi et al., 2023), evaluating security threats can be highly disruptive on live systems, thus advising the use of laboratory environments. However, when such environments are not available, an alternative is to resort to interactive platforms enabling the creation of entirely virtual representations (called scenarios) of existing railway infrastructures, emulating their operations by exploiting virtualization and digital twin technologies. This approach can reduce setup and running costs, allowing for multiple scenarios to be remotely accessible and evaluated in parallel. It should be mentioned that, regardless of the chosen approach, one of the challenges to reproduce the complexity of the setup deployed in the field is to obtain highly detailed knowledge from the system owners about their systems.

The aforementioned platforms can be classified into two main types: simulation-based and emulation-based architectures. The main difference is that an emulation environment reproduces with great accuracy the system peculiarities, while simulation mimics the essential characteristics of the physical system but may not replicate some of its minor details – something which may be relevant for network security. Finally, hybrid scenarios combining virtual and real devices may also constitute a suitable alternative, especially for cases where some legacy systems cannot be virtualized (Foglietta et al., 2018).

Table 2 presents a comparison between some of the well-known virtual test platforms. It should be mentioned that these can also be leveraged to implement railway infrastructure scenarios, allowing for instance to study the impact of attacks on the IxL to ATS conduit, to understand how malware can propagate through the network or to test a specific Layer 2 attack. Another benefit of using test platforms is the possibility to resort to automation tools such as Ansible, streamlining the provisioning and configuration of complex setups.

Table 2: A SCHEMATIC COMPARISON BETWEEN SOME WELL-KNOWN VIRTUAL TEST SOLUTIONS (Soderi et al., 2023)

	CORE (US NRL, n.d.)	**Mininet (Mininet, n.d.)**	**EVE-NG (EVE, n.d.)**	**GNS3 (Solarwinds, n.d.)**	**Cisco CML (Cisco., n.d.)**
Network configuration	Python, Labs	Python, CLI	API, LABS	API, Labs	API, Labs
Network emulation level	L3, (L1/L2 EMANE)	L2	L2	L2	L2
Node operating system emulation	No	No	Yes	Yes	Yes
Licensing	BSD	BSD	GPL, Commercial	GPL	Commercial

Cyber threats can have many root causes, ranging from weak configurations to inappropriate security controls, among many others. Thus, one major advantage of using virtual test platforms is to allow security teams to assess the impact of specific threats in a way that it would be hard or even impossible to perform on a full physical environment, also allowing to safely use techniques and tools that could potentially have a disruptive impact in production environments.

Following the cyber kill chain (Lockheed Martin, n.d.), the steps for using this kind of approach to evaluate the network security would be the following: to emulate the network with the same configurations as the field devices; search for vulnerabilities using automated scanning tools like Nessus (Tenable, n.d.); and, finally,

enumerate the found vulnerabilities and measure their impact. Based on the identified vulnerabilities, we can now move on to develop and test countermeasures.

4.3.4 Testbed

Another approach to replicate the IxL to ATS conduit, is presented in the work of (Heinrich et al., 2020) , which describes a laboratory environment testbed, depicted in Figure 2. This scenario uses a centralised architecture with object controllers, as well as simulators for the light signals and track changing point machines. Object controllers are based on Raspberry Pi single board computers. Such object controllers are part of modern, modularised computer-based interlocking systems, whose function is to receive command and control messages via a communication network and set the controlled field element (light signal, point) to the commanded state. (Heinrich et al., 2020). A graphical user interface (GUI) was also implemented, allowing to set routes between two signals.

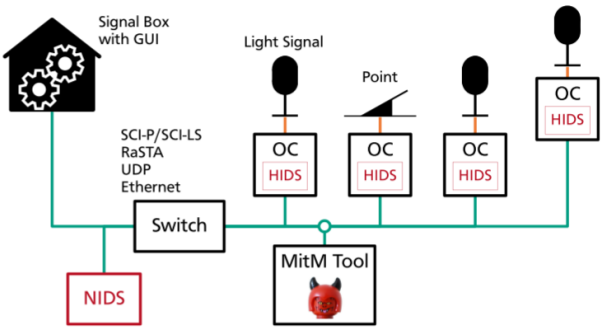

Figure 2: Overview of the testbed's architecture and components (Heinrich et al., 2020)

This scenario gives the security researcher the opportunity to test and implement security controls, and at the same to simulate realistic attacks. In this specific case a man in the middle attack was also demonstrated, by performing ARP spoofing and intercepting and changing the datagrams.

5. Conclusions

This article provides a high-level overview of the railway environment, detailing its societal importance and susceptibility to cyber-attacks. It explores the challenges of harmonising cybersecurity controls, stemming from the stark contrast between cutting-edge systems and those reliant on 1980s technology. Additionally, it outlines the organisation of the European guideline TS50701, tailored for railway cybersecurity. The paper also discusses applicable standards and guidelines not specifically aimed at railways. Furthermore, it examines a critical aspect of railway infrastructure and ongoing efforts to mitigate associated risks through risk assessment tools and methodologies. Lastly, it explores virtual test platforms and testbeds, demonstrating their current capabilities in testing new solutions against cyber threats.

Future developments will encompass a deeper analysis of existing security assessment guidelines, as well as an overview of the contact points between TS50701 and national regulations, such as the US Transportation Security Administration's Security Directive 1580-21-01 (US Transportation Security Administration, 2021). Another interesting line for future work is the comparative analysis of existing standards with the upcoming IEC 9/PT 63452 (International Electrotechnical Commission, 2013).

Acknowledgements

This work was partially funded by National Funds through the FCT -- Foundation for Science and Technology, I.P., and the European Social Fund, through the Regional Operational Program Centro 2020, within the scope of the project CISUC UID/CEC/00326/2020. It was also co-funded by the "Agenda Mobilizadora Sines Nexus" project (ref. No. 7113), supported by the Recovery and Resilience Plan (PRR) and by the European Funds Next Generation EU, following Notice No. 02/C05-i01/2022, Component 5 – Capitalization and Business Innovation – Mobilising Agendas for Business Innovation.

References

Adamos, K., Stergiopoulos, G., Karamousadakis, M., Gritzalis, D., 2024. Enhancing attack resilience of cyber-physical systems through state dependency graph models. Int J Inf Secur 23, 187–198. https://doi.org/10.1007/s10207-023-00731-w

Cardoso, A. and Simões, P., 2011. Cloud computing: Concepts, technologies and challenges. In: proc. of the International Conference on Virtual and Networked Organizations, Emergent Technologies, and Tools (ViNOrg 2011). doi: 10.1007/978-3-642-31800-9_14

Barrett, M., 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.04162018

Castanier, B., Cepin, M., Bigaud, D., Berenguer, C., Okstad, E.H., Bains, R., Myklebust, T., Jaatun, M.G., 2021. Implications of Cyber Security to Safety Approval in Railway. Research Publishing. https://doi.org/10.3850/981-973-0000-00-0

CENELEC, 2017. CENELEC EN 50126 - Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) . ISBN: 9780539085266

CENELEC, 2021. CLC/TS 50701 - Railway applications-Cybersecurity.

CENELEC, 2023. CLC/TS 50701:2023 - Railway applications-Cybersecurity. ISBN: 9780539208559

Cisco Systems Inc, CML - Cisco Modeling Labs [WWW Document], n.d. URL: https://developer.cisco.com/modeling-labs/ (accessed 2.13.24).

CYRail consortium, 2018. CYRail recommendations on cybersecurity of rail signalling and communication systems. UIC-ETF. URL: https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf (accessed 2.16.24).

Foglietta, C., et al., 2019. From Detecting Cyber-Attacks to Mitigating Risk Within a Hybrid Environment. IEEE Systems Journal, vol. 13, no. 1, pp. 424-435. doi: 10.1109/JSYST.2018.2824252.

Liveri, D., Theocharidou, M., Naydenov, R., ENISA, 2020. RAILWAY CYBERSECURITY Security measures in the Railway Transport Sector NOVEMBER 2020 RAILWAY CYBERSECURITY ABOUT ENISA. https://doi.org/10.2824/235164

DIN, 2015. DIN VDE V 0831-104 VDE V 0831-104:2015-10 - Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443 [WWW Document]. DIN VDE V 0831-104 VDE V 0831-104:2015-10. URL https://www.vde-verlag.de/standards/0800264/din-vde-v-0831-104-vde-v-0831-104-2015-10.html (accessed 2.16.24).

EVE-LG Ltd, n.d. EVE - The Emulated Virtual Environment For Network, Security and DevOps Professionals. [WWW Document], n.d. URL https://www.eve-ng.net/ (accessed 2.13.24).

Freitas, M., Rosa, L., Cruz, T., Simões, P., 2019. SDN-Enabled Virtual Data Diode. In: proc. of the 4th ESORICS Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS 2018). doi: 10.1007/978-3-030-12786-2_7

Gaspar, J., Cruz, T., Lam, C.-T., Simões, P., 2023. Smart Substation Communications and Cybersecurity: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2456-2493. doi: 10.1109/COMST.2023.3305468

Gordeychik, S., 2019. Cyber Resilience of Railway Signalling Systems - Academia.edu [WWW Document]. URL https://www.academia.edu/40629914/Cyber_Resilience_of_Railway_Signaling_Systems (accessed 2.16.24).

Heinrich, M., Arul, T., Katzenbeisser, S., 2020. Demo: Railway Signalling Security Testbed, in: IEEE Vehicular Networking Conference, VNC. IEEE Computer Society. https://doi.org/10.1109/VNC51378.2020.9318338

International Electrotechnical Commission., 2013. IEC 62443-3-3. Industrial communication networks--network and system security. Part 3-3, System security requirements and security levels.

International Electrotechnical Commission, 2023. PT 63452 ED1 - Railway applications - Cybersecurity.

International Organization for Standardization, 2013. Standard ISO/IEC 27001 - Information Technology—Security Techniques—Information Security Management Systems—Requirements. Standard ISO/IEC 27001.

International Organization for Standardization, 2018. IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

International Organization for Standardization, 2022. ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls [WWW Document]. International Organization for Standardization. URL https://www.iso.org/standard/75652.html (accessed 2.16.24).

Lockheed Martin [WWW Document], n.d. Cyber Kill Chain. URL https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed 2.13.24).

Kapoor, N., 2022. Understanding Railway Cybersecurity [WWW Document]. International Society of Automation - ISA Global Cybersecurity Alliance. URL https://gca.isa.org/blog/understanding-railway-cybersecurity (accessed 2.16.24).

Malatras, A., Stanic, Z., Lella, I. (2023). ENISA threat landscape: transport sector (January 2021 to October 2022): March 2023, (A. Malatras, editor ,Z. Stanic, editor,I. Lella, editor, R. De Sousa Figueiredo, editor, E. Tsekmezoglou, editor, M. Theocharidou, editor, R. Naydenov, editor, A. Drougkas, editor), ENISA. https://data.europa.eu/doi/10.2824/553997

Mayor of London, 2022. What we do - Transport for London [WWW Document]. Mayor of London. URL https://tfl.gov.uk/corporate/about-tfl/what-we-do (accessed 2.16.24).

Mininet Project. [WWW Document], n.d. URL http://mininet.org/ (accessed 2.13.24).

Parkinson, H.J., Basher, D.R., Bamford, G., 2023. Railway cyber security and TS50701, in: Proceedings of the Fifth International Conference on Railway Technology: Research, Development and Maintenance. Civil-Comp Press, pp. 1–9. https://doi.org/10.4203/ccc.1.17.1

Prochazka, J., Novobilsky, P., Prochazkova, D., Valousek, S., 2023. Cybersecurity Design for Railway Products. Research Publishing Services, pp. 304–311. https://doi.org/10.3850/978-981-18-5183-4_r09-01-099-cd

Rail Industry Safety and Standards Board, 2018. AS 7770:2018 Rail Cyber Security. ISBN: 9781760720780

Rosa, L., Alves, P. , Cruz, T., Simões, P., Monteiro, E., 2015. A Comparative Study of Correlation Engines for Security Event Management. In: proc. of the 10th International Conference on Cyber Warfare and Security (ICCWS-2015).

Siemens, 2022. Infrastructure in the Cloud - Digital Offerings for rail infrastructure [WWW Doc]. Siemens. URL: https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/infrastructure/infrastructure-in-the-cloud.html (accessed 2.16.24).

Soderi, S., Masti, D., Lun, Y.Z., 2023. Railway Cyber-Security in the Era of Interconnected Systems: A Survey. IEEE Transactions on Intelligent Transportation Systems 24, 6764–6779. https://doi.org/10.1109/TITS.2023.3254442

Solarwinds Worldwide, GNS3 (Graphical Network Simulator-3). [WWW Document], n.d. URL https://www.gns3.com/ (accessed 2.13.24).

Stouffer, K., 2023. Guide to Operational Technology (OT) Security. https://doi.org/10.6028/NIST.SP.800-82r3

Tenable, Inc., Nessus Vulnerability Scanner [WWW Document], n.d. URL https://www.tenable.com/products/nessus (accessed 2.13.24).

Thomas, R.J., Chothia, T.; Ordean, M., 2022. Cyber security in the rail sector-an integrated approach. Birmingham.

UK Government, 2023. Cyber Essentials scheme: overview - GOV.UK [WWW Document]. URL https://www.gov.uk/government/publications/cyber-essentials-scheme-overview (accessed 2.16.24).

UK Government, 2018. The Network and Information Systems Regulations, S.I. 2018/506. URL: https://www.legislation.gov.uk/uksi/2018/506/contents/made (accessed 2.16.24).

U.S. Department of Homeland Security, 2022. U.S. department of homeland security-transportation security administration, security directive 1580/82-2022-01 - rail cybersecurity mitigation actions and testing.

US Navy Research Laboratory, CORE - Common Open Research Emulator [WWW Document]. URL: https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/CORE (accessed 2.13.24).

US Transportation Security Administration, 2021. Security Directive 1580-21-01 - Enhancing Rail Cybersecurity [WWW Document]. URL: https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf (accessed 10.4.24).

Winter, P., 2009. Compendium on ERTMS. Hamburg, Eurail Press. ISBN-10: 3777103969.