The Fifth International Conference on Railway Technology
RAILWAYS 2022
22–25 August 2022
Montpellier, France

Proceedings of the Fifth International Conference on
Railway Technology:
Research, Development and Maintenance
Edited by J. Pombo
Civil-Comp Conferences, Volume 1, Paper 17.1
Civil-Comp Press, Edinburgh, United Kingdom, 2022, doi: 10.4203/ccc.1.17.1

Railway cyber security and TS50701

H.J. Parkinson[1], D.R. Basher[1] and G. Bamford[2]

[1]Digital Transit Limited
[2]Advisory Limited

Abstract

The operational technology cyber security (OTCS) of rail systems is lagging behind other industries such as aviation [1]. For this short paper, standards, guidance and research papers including the new CENELEC technical specification TS50701 [2] were reviewed. Gaps in the coverage of this literature were identified, as well as further work that needs to be done to ensure the railway becomes more cyber secure in the future.

Keywords: cybersecurity, TS50701, railway, safety

1 Introduction

Control systems that are not secure against cyber-attacks are vulnerable, and cannot be considered safe. In other words, “If it is not secure then it is unlikely to be safe” [3]. The relationship between cybersecurity and functional safety is outlined in Figure 1.

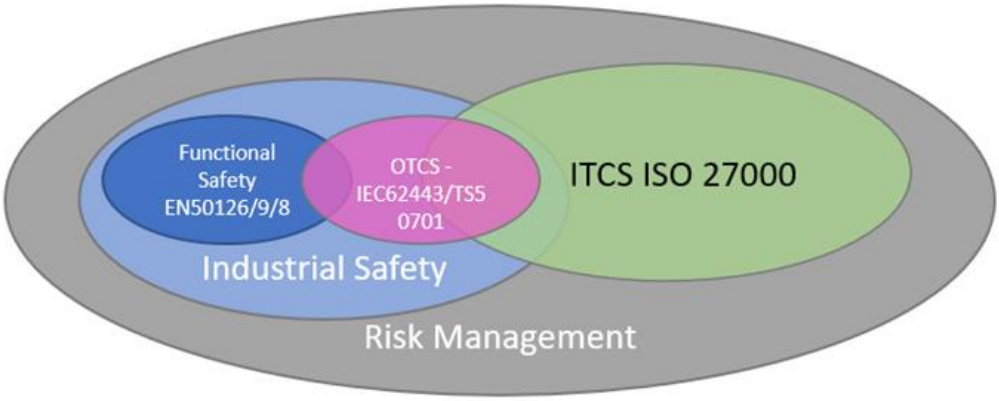

Figure 1. Relationship between cybersecurity and safety

Rail is similar to other industries in terms of safety regulation; however, it is unique in terms of cybersecurity as it consists of extensive business premises that are widely accessible to the public with infrastructure that can span entire countries or continents.

ITCS (Information Technology Cyber Security) has been managed in rail with the adoption of the ISO27000 [4] suite of standards, and in this way, railway business systems are not too dissimilar to other industries. However, OTCS (Operational Technology Cyber Security) rail systems are lagging behind other industries such as aviation [1] and could be vulnerable to attack. Figure 2 shows the demarcation between OTCS and ITCS as described in TS50701 [2].

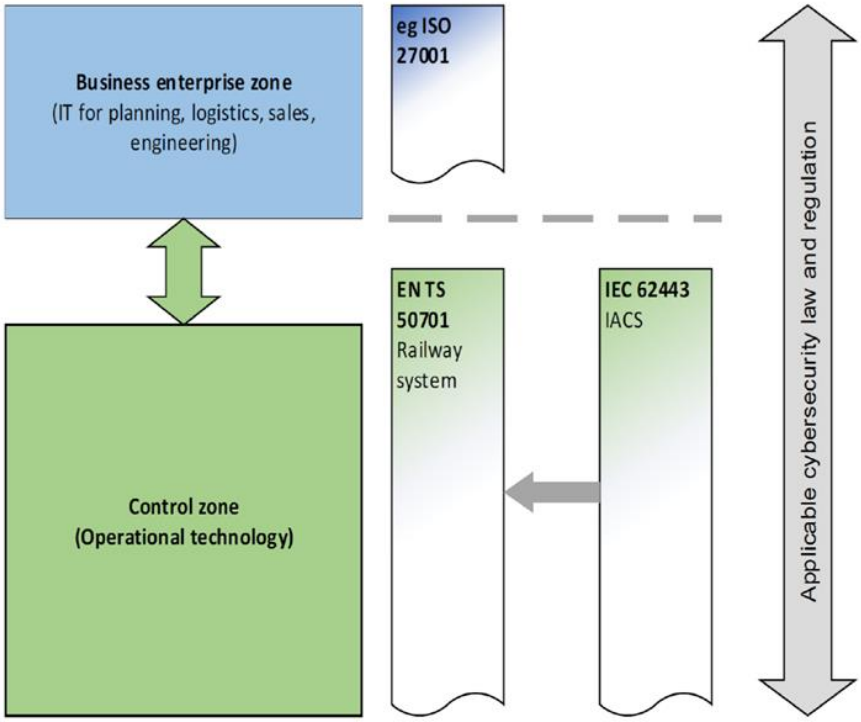

Figure 2. OTCS (green) and ITCS (blue) relationship according to TS50701 [2]

To help understand why cyber security in rail systems is lagging behind other industries, it is important to consider the complex threat landscape that exists on the railways. The railway has a substantial amount of technology that is specific to the rail domain. These systems can have operational lifetimes of 30 or more years [1]. Additionally, as digitalisation of the railway continues, the threat surface will only continue to grow. This digitalisation is coming about through implementation of new technologies, many of which are commercial off the shelf (COTS) and bring with them an increased chance of exposure to a cyber-attack [5]. Because of the long lifetime of rail systems, most existing systems are legacy systems, which were not designed with the modern understanding of cyber security in mind [6].

This complexity can be navigated by following standards and industry research. This paper aims to define the state of the art in OTCS via a comprehensive review of research and standards, identifying gaps that are not being covered by the literature. Filling these gaps could help create more robust standards which can be followed.

Section 2 of the paper describes methods for selecting and analysing the materials, Section 3 provides the output from the literature and standard reviews and identifies the coverage. Section 4 provides a conclusion clearly identifying areas that require further research.

2 Methods

The literature review was split up into two sections. The first section covered standards and guidance and the second covered published research papers. The reason for this demarcation was that the intent of research is to explore the state of the art, whereas the purpose of standards is to provide guidance and both normative and informative structure to facilitate the implementation of cybersecurity.

The criteria for an item to be included in standards and guidance assessment were that it had to be either a published standard or guidance from a public body or institution. The research papers were generally taken from available journals or conferences.

A thorough literature review was carried out on the standards and guidance. It was determined whether they focused on OTCS, ITCS or both; whether they specifically discussed (and not just referenced) the EN50126 [7] standard; whether they were railway focused, and whether they could be applied internationally.

For the selection of papers, various research portals were searched. The guide words “cybersecurity” and “rail/railway/railroad” were used for finding relevant papers. This literature review specifically targeted recent papers that covered how OTCS cybersecurity is being applied in the railway. The papers were analysed, and the key

focuses of each were determined. These could fall into one or more of the following categories:

- Tools and techniques – Methods for testing and ensuring cybersecurity
- Lifecycle – Links to the 'EN50126 Lifecycle'
- Case Study – An example of the application of a standard, method or system
- Literature Review/Overview
- Financial Aspects – Information regarding the financial cost of implementing Cybersecurity

Additionally, any standards or systems that were mentioned and relevant to the paper were recorded, as well as whether the paper focused on ITCS, OTCS or both.

3 Results

Table 1 presents the findings from the review of standards and guidance.

Standards/ Guidance Reference	Mainly OTCS Focused	Mainly ITCS Focused	Covers ITCS and OTCS	References Links to EN50126 Lifecycle	Railway Focused	International Focus
ISO27001 [4]		✓				✓
NIST Cybersecurity Framework [8]			✓			
NIST SP800-82 [9]	✓					
NIS Regs [10]			✓			✓
Cyber Essentials [11]		✓				
AS 7770 [12]			✓		✓	
IEC 62443 [13]	✓					✓
DIN VDE V 0831-104 [14]	✓				✓	
TS50701 [2]	✓			✓	✓	✓
CYRail D7.5 [15]	✓				✓	✓

Table 1 - Comparison of Cyber Security Standards and Guidance

From our literature review of published research, we have classified the content and aims of the various papers as shown in Table 2.

Papers	Focuses					IT or OT	Standards	Systems Covered
	Tools and Techniques	**Lifecycle**	**Case Study**	**Lit Review / Overview**	**Financial Aspects**			
Ciancabillet al. [16]		Left hand side of EN50126 V	Application of TS50701			OT	TS50701	Train Integrity
Procházka et al. [17]	MILS – Multiple Independent Levels of Security					OT	TS50701 IEC 62443 IEC 61375 2-6 IEC 15408	Train Communication Gateway
Gabriel et al. [18]	RiKoV Method			ERTMS security flaws		IT/OT	ISO/IEC 9797-1 ERTMS	ERTMS
Ozerov [19]				General Overview of SOTA		IT/OT	ISO27001 IEC 62443	
Chothia et al. [20]	Cryptographic Analysis of ERTMS protocols		A theoretical attack on the EURORadio.			OT	ERTMS	ERTMS EURORadio
Schlehuber et al. [21]	'Shell' Concept			Overview of signalling cyber security and the interaction with safety		OT	NIS Regulations ISO 27000 IEC 62443 DIN VDE V 0831-104 EN 50126/9	Signalling Systems
Pawlik [22]	SSIRM - Safety and security impact reference model			Discussion of safety and security interactions		OT	EN50126	
Liu et al. [23]	Streamlined risk assessment		Case Study of three use cases – ATCS, Remote Rail Bridge control and Positive train control			IT/OT	NIST Cybersecurity Best Practise	ATCS Remote-Controlled Rail Bridges PTC
Rekik et al. [24]	ETSI TS 102 165-1 V4.2.3		Application of IEC 62443			OT	IEC 62443	External Door Control
Pizzi [25]	Fault tree analysis		Vulnerabilities in Wheel Slide Protection (WSP)			OT	EN50126 IEC 61025	Brakes

Kour, et al. [26]				Statistical Analysis of Cybersecurity incidents in rail.	Briefly mentions budgets	IT/OT		Maintenance Systems
Cébulski et al. [27]				Report on the state of the art in cybersecurity rail		IT/OT		
Matta et al. [28]	Using a risk management framework Creating a IOT framework architecture Seperaton Kernal STRIDE	Risk assessment				IT/OT	IEC 62443 3-3	IoT based systems
Unwin, et al [29]	A technique to identify attack scenarios via war gaming approach					IT/OT		Generic Railway Control System
Boss [5]			ERTMS	State of the art analysis with comprehensive lit review and guidance on communication between signalling and security engineers		IT/OT		ERTMS
Heinrich et al. [30]	MILS approach and security requirements engineering process (DIN VDE V 0831-104)		CCS			OT	IEC 62443 DIN VDE V 0831-104	Signalling Systems (CCS)
Bloomfield et al. [6]	Systematic analysis of Specification and cybersecurity risk management	Left hand side of V covered plus testing	ERTMS Level 2			OT		ERTMS
Braband [31]	Evaluation of Threat and Risk Analysis / Matrices					IT/OT	EN50126 IEC 62443 IEC 15408 ISO27005	

Table 2 – Research Paper Review Findings

There are several comprehensive literature reviews available, in particular Boss [5]. Only a few papers analysed the detailed lifecycle processes for ensuring OTCS in rail [5][21][24] using, for example, IEC 62443 [13] and DIN VDE V 0831-104 [14]. Ciancabilla [16] has specifically provided a case study that looks at the application of the TS50701 processes so far, although this was primarily the risk assessment phase.

Reviewing previous rail cyber-attacks case studies or staged cyber-attacks on the railway helps to establish why better cybersecurity standards may be needed. There are several papers documenting railway specific incidents, the most comprehensive being Kour [26] which also provides a statistical review of cybersecurity incidents in the railway. Primarily, the papers reviewed covered ITCS incidents. It is important to note that a large-scale attack on railway OT has never been reported (other than a supposed attack in Lodz on trams [32]), however there have been sophisticated and successful OTCS attacks on industrial PLCs in Iran's Nuclear Enrichment program [26]. As political tensions continue to increase, the risk of a cyber-attack by state sponsored actors continues to grow. Whereas independent hackers choose simple attacks which provide large monetary rewards, state actors are more likely to target critical infrastructure [29].

4 Conclusions and Contributions

The review of the standards and guidance in Table *1* enabled us to make the following four conclusions and observations.

1. The IEC 62443 family of standards and guidance provides comprehensive guidance on securing control systems and are applicable internationally. However, the railway has many unique features that require specialised requirements, specifically the distributed nature and the complicated ownership model that the railway employs, that IEC 62443 does not consider. TS50701 now fills this gap in coverage.

2. DIN VDE V 0831-104 is a German pre-standard, which is more restrictive in its coverage compared to TS50701 applying to German signalling systems. The experience of using this standard should inform further development of TS50701.

3. From our analysis of standards, only TS50701 covers generic rail OTCS and linkage to the EN50126 lifecycle. TS50701 is a key tool for OTCS because it gives a sound basis to:

- Perform risk assessment,
- Review railway architecture
- Enable zone models and conduits to be constructed and analysed with communication protocols established
- Demonstrate tolerable security risks
- Produce a cybersecurity case, satisfying all the stakeholders

4. The review has confirmed IEC 62443 as the definitive OTCS industry standard, and in combination with TS50701 provides a firm basis for securing rail systems.

From the research paper literature review, we have three main findings.

5. Our analysis of the literature showed that little consideration has been given to the financial cost of cyber security in the rail industry. Fully securing the expansive rail network has huge cost implications that need to be considered. Operators and asset owners need to weigh the risk of implementing cyber security against the costs of an incident, which could be loss of service, a data breach or even loss of life. Much like safety, it may seem expensive to secure the railway, but that cost can pale in comparison to the cost of an accident.

6.There was no evidence that the research sufficiently identifies the consequences of cyber-attacks for use in a risk assessment. In comparison safety risk assessments have access to clearer consequences for accidents [7]

7. To help improve TS50701, further case studies are required on its application. It needs further work before it becomes an Euronorm.

References

[1] ENR135 – V1 – Taking cybersecurity challenges into account in railway safety
[2] CLC/TS 50701:2021 - Railway applications – Cybersecurity
[3] Department for Transport, “Rail Cyber Security Guidance to Industry,” 2016.
[4] ISO/IEC 27000:2018 Information Security Management
[5] J. Boss – Railway Signalling and Cyber Security
[6] Bloomfield R., et al - The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective
[7] EN50126-1: Railway Applications - The Specification and Demonstration of RAMS 2017.
[8] NIST Cybersecurity Framework
[9] NIST SP800-82 CSRC - https://csrc.nist.gov/publications/sp800
[10] Security of Network & Information Systems Regulations (NIS Regulations) 2018
[11] Cyber Secure Scheme https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[12] AS 7770 - Rail Cyber Security – RISSB Australia.
[13] IEC62443 Suite of Standards
[14] DIN VDE V 0831-104:2015-10 Electric signalling systems for railways - Part 104: IT Security
[15] CYR-WP7-D-CNC-004-01_-_D7.5_Recommendations_Brochure
[16] Attilio Ciancabilla et al, Application of FprTS 50701 ENISA-ERA Conference: Cybersecurity in Railways
[17] Procházka et al. (2020). Cybersecurity of Railway Network Management and Partitioning. Problemy Kolejnictwa - Railway Reports.
[18] Alexander Gabriel et al. (2018). The determination of critical components of European Rail Traffic Management systems towards cyber-attacks.
[19] Ozerov, A., 2020. Cybersecurity of Railway Command and Control Systems.

[20] T. Chothia et al., “A Formal Security Analysis of ERTMS Train to Trackside Protocols Chothia”
[21] C. Schlehuber et al. “Challenges and Approaches in Securing Safety-Relevant Railway Signalling,”
[22] Marek Pawlik, “Concept of the railway safety, security and cybersecurity functional integrity levels”
[23] Federal Railroad Administration, 2020. Cyber Security Risk Management for Connected Railroads. Technical Reports.
[24] M. Rekik et al. “Cyber-physical security risk assessment for train control and monitoring systems,”
[25] Pizzi, G., 2020. “Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment”
[26] Kour, R. (2020). Cybersecurity in Railway : A Framework for Improvement of Digital Asset Security
[27] European Union Agency for Railways, 2021. Taking cybersecurity challenges into account in railway safety.
[28] Matta, G et al. 2021. “Risk Management and Standard Compliance for Cyber-Physical Systems of Systems”
[29] Unwin D et al. “Railway cyber safety: An intelligent threat perspective”
[30] Markus Heinrich et al., “Security Requirements Engineering in Safety-Critical Railway Signalling Networks”
[31] Jens Braband. “Towards an IT Security Framework for Railway Automation”
[32] https://www.theregister.com/2008/01/11/tram_hack/#:~:text=A%20Polish%20teenager%20allegedly%20turned,in%20one%20of%20the%20incidents.