Gaggero *et al. J Surveill Secur Saf* 2024;5:52-61
DOI: 10.20517/jsss.2023.35

Journal of Surveillance, Security and Safety

Original Article

Open Access

A survey on wireless-communication vulnerabilities of ERTMS in the railway sector

Giovanni Battista Gaggero, Mario Marchese, Paola Girdinio

Department of Electrical, Electronic and Telecommunications Engineering, and Naval Architecture (DITEN) University of Genoa, Genoa 16145, Italy.

Correspondence to: Dr. Giovanni Battista Gaggero, Department of Electrical, Electronic and Telecommunications Engineering, and Naval Architecture (DITEN) University of Genoa, Via all'Opera Pia 11A, Genoa 16145, Italy. E-mail: giovanni.gaggero@edu.unige.it; ORCID: 0000-0001-6404-2451

How to cite this article: Gaggero GB, Marchese M, Girdinio P. A survey on wireless-communication vulnerabilities of ERTMS in the railway sector. *J Surveill Secur Saf* 2024;5:52-61. http://dx.doi.org/10.20517/jsss.2023.35

Received: 26 Oct 2023 **First Decision:** 21 Dec 2023 **Revised:** 5 Jan 2024 **Accepted:** 18 Feb 2024 **Published:** 25 Feb 2024

Academic Editor: Enrico Zio **Copy Editor:** Yanbin Bai **Production Editor:** Yanbin Bai

Abstract

Railways represent a critical infrastructure in modern societies. In the past few years, cyber attacks on these infrastructures have been rising, and there is a need to properly analyze the vulnerabilities of field devices. This work focuses on the wireless communication that is defined in the European Rail Traffic Management System standard and proposes a survey of the vulnerabilities of the main employed protocols. Also, it provides some research lines. This study shows how several issues still exist within wireless communication in the railway sector.

Keywords: Railways, wireless communication, cybersecurity, critical infrastructures, ERTMS, GSM-R

1. INTRODUCTION

The railway industry has historically been a pillar of transportation infrastructure, facilitating the movement of goods and people across vast distances with remarkable efficiency. In the modern age of digital connectivity, the global railway sector has undergone a profound transformation. The integration of advanced technologies has not only enhanced the efficiency and safety of rail systems but has also exposed them to an unprecedented level of cybersecurity threats. As railways rely increasingly on digital systems, the protection of the availability of infrastructure and passenger safety has become contingent upon robust cybersecurity measures. The Eu-

ropean Rail Traffic Management System (ERTMS), developed by the European Union (EU) as a standardized system for managing train traffic and control, represents one of the most significant advancements in railway technology. It integrates real-time data communication and signaling, ensuring safe and efficient operations across European railways. Nonetheless, as this system relies heavily on digital technology, it also opened a Pandora's box of cybersecurity vulnerabilities. Recent years have seen a surge in cyberattacks targeting the railway sector. These attacks have ranged from disruptive ransomware incidents to more sophisticated and potentially catastrophic threats that could compromise the safety of passengers and freight transportation. Real-world cases, such as the 2015 attack on Ukraine's power grid, which demonstrated the ability of malicious actors to disrupt critical infrastructure, serve as stark reminders of the looming threats faced by the railway industry. This paper explores the emerging cybersecurity issues in the railway sector, with a particular focus on the ERTMS standard, and highlights real-world cases of cyberattacks that have raised concerns about the security of rail networks. This paper delves into the multifaceted issues surrounding railway cybersecurity, including the vulnerabilities inherent in the ERTMS standard, the potential consequences of successful cyberattacks, and the evolving threat landscape. It also offers insights into the strategies and solutions that can be employed to safeguard railway systems, protect passenger safety, and ensure the continued resilience of this critical transportation infrastructure in the face of cyber threats.

The paper is structured as follows. Section 2 analyzes the related works that analyze and survey the issue of cybersecurity issues in railways' wireless communication. Section 3 introduces the ERTMS standard for signaling in the railway environment in all of its parts, including the Global System for Mobile Communications for Railways (GSM-R), and analyzes the landscape of cybersecurity standards that specifically address the sector. Sector 4 discusses the main issues that are present in railway wireless communication, taking into account two main channels: cellular communication and the communication between the balise and the onboard system. Finally, in Section 5, conclusions are drawn.

2. RELATED WORKS

In the past few years, due to the general rise of attacks toward critical infrastructures, including railway systems, the number of publications that specifically take into account the issue has been increasing. Teo *et al.*[1] presented SecureRails, an open-source simulator designed for analyzing cybersecurity in railway systems, that is composed of two components: a train motion simulator developed on the OpenRails platform and a model-based railway traction power flow simulator created using Matlab, which interact throughout their simulation runtime using the JSON-RPC protocol. The platform can be used to assess the impact of an attack but does not take into account the actual implementation of attacks. Wang and Liu[2] developed a risk management methodology for cybersecurity in railway Cyber-Physical Systems, and performed a retrospective case study on the Advanced Train Control System (ATCS), which is currently operational in numerous railways across the United States. López-Aguilar *et al.*[3] present a literature review on information security and privacy within railway transportation systems, following a methodology introduced in state of the art, and suggest some research lines to be followed.Soderi *et al.*[4] present a survey that delves into the cybersecurity aspects of railway systems, examining industry standards, guidelines, frameworks, and technologies employed to assess and mitigate cybersecurity risks. In particular, the paper puts emphasis on signaling, which heavily relies on computer and communication technologies. The study also analyzes practical approaches and tools available to practitioners in enhancing the cybersecurity process, including cyber ranges, which serve as a crucial tool for modeling and simulating computer networks and attack-defense scenarios. While this represents the most complete work in the state of the art, it lacks analysis regarding, in particular, attacks between the Onboard systems and Balises. Ai *et al.*[5] discuss the main challenges for wireless communications for high-speed railways, taking into account the evolution of cellular technologies but not addressing the issue of cybersecurity. The security aspects of wireless communication in railway systems are one of the topics that have been less investigated in the state-of-the-art field of railway security.

Table 1. Real-world cyberattacks that effectively stopped train operation

Year	Description	Ref.
2003	A cyber attack targeting the CSX Transportation headquarters in Florida disrupted signaling across thousands of kilometers of railway lines. This event has been widely known as the "Sobig" incident	[6]
2008	A young individual manipulated the train network in Lodz, Poland, leading to the derailment of four tram vehicles and causing injuries to twelve people	[7]
2012	A cyber assault on the computer systems of a rail company in the Northwestern United States disrupted railway signals for a period of two days	[8]
2016	The systems of a well-known Ukrainian rail company were infected by the BlackEnergy and KillDisk malware. In December 2015, the Ukraine power grid cyberattack was also targeted using the same malware	[9]
2021	A cyberattack on Iran's railroad system caused several issues across the whole country	[10]
2022	In the context of the conflict between Russia and Ukraine, the Belarus trains toward Russia have been stopped due to a cyberattack	[11]
2023	Hackers stopped 20 trains in Poland with a simple radio-stop message broadcasted with a cheap apparatus	[12]

2.1. Real attacks

Following the path of many critical infrastructures, the railway environment has already suffered from successful cyberattacks in the past, and both the number and complexity of these attacks have been increasing in the last few years. Table 1 reports only the main real attacks that effectively interrupted the operation of the infrastructure.

It can be noticed that few of them are related to wireless vulnerabilities; this is probably because, in the past, the railway sector had vulnerabilities that were much more easily exploitable. In particular, control networks in the railway environment present important similarities with other industrial control systems. Therefore, they present the same vulnerabilities: for example, incidents such as those in [6], [8] and [9] are related to attacks directly targeting control rooms through traditional attacks such as Ransomware, which indirectly affects the transportation availability. The protection against these attacks involves the use of general standards and guidelines for the cybersecurity of industrial control systems, such as IEC 62443. Nevertheless, as the sector is putting in place cybersecurity countermeasures, also the attack complexity is increasing. For example, the most recent attack mentioned is based on a simple radio-stop message broadcasted with a cheap apparatus [12]. The relatively low sophistication of this attack suggests that this kind of incident is going to increase in the next few years.

3. STANDARDS

3.1. ERTMS

The ERTMS comprises a set of standards designed to manage and facilitate signaling operations across railways within the EU. The EU Agency for Railways (ERA) is the organizational umbrella for the development of these standards. ERTMS primarily focuses on promoting interoperability among trains in the EU. Its objectives include significantly improving safety measures, optimizing the efficiency of train transportation, and fostering cross-border interoperability of rail transport across Europe. This is achieved by replacing previous national signaling equipment and operational protocols with a unified Europe-wide standard for train control and command systems. To achieve these goals, the ERTMS standard includes the following parts [13]:

- GSM–R (communication): The system is an international wireless communications standard specifically designed for railway communication and applications, operates as a sub-system within the ERTMS, and facilitates communication between trains and railway regulation control centers. It is built upon the GSM and EIRENE – MORANE specifications, ensuring reliable performance even at high speeds of up to 500 km/h (310 mph) without any communication loss. It is worth noting that GSM-R could potentially be replaced by LTE-R in the future. The UIC's Future Railway Mobile Communication System (FRMCS) program is exploring the possibility of transitioning to a "5G"-based system, specifically 3GPP R15/16, which would

skip two technological generations.

- European Train Control System (ETCS, signaling): The operation management level is aimed at optimizing train movements through the ”intelligent” interpretation of timetables and train running data. This process involves enhancing real-time train management, route planning, rail node fluidity, and providing pertinent information to both customers and operating staff.
- European Train Management Layer (ETML, payload management): the European Train Control System (ETCS) serves as the signaling component of the system, encompassing the control of movement authorities, automatic train protection, and the interface to interlockings. It facilitates the gradual simplification of tasks for train drivers by automating control activities. ETCS brings trackside signaling directly into the driver's cabin, providing essential information on the onboard display. This system enables continuous train control, allowing the train driver to focus on core tasks while ensuring safe and efficient train operations.

At its core, ETCS functions through two main components, as shown in Figure 1: the trackside equipment and the onboard system. Trackside ETCS equipment consists of balises, which are transponders placed alongside railway tracks at specific intervals. These balises communicate with passing trains, transmitting vital information such as speed limits, track configurations, and signaling aspects. Additionally, Eurobalises, a specific type of balise used in ETCS, can also send movement authorities, which dictate how far a train can travel and at what speed. Trackside equipment also includes Radio Block Centers (RBCs), which manage train movements and issue movement authorities to trains within their jurisdiction. Onboard ETCS equipment is installed in trains and consists of a computer-based control unit, a digital map of the railway network, and a display for the train driver. The onboard system continuously receives information from trackside balises and the RBCs via radio communication. Based on this data, the onboard system calculates and displays essential information to the train driver, including speed limits, upcoming signals, and any movement authorities received from the trackside equipment. If the train approaches a section of track too fast or violates any signaled restrictions, the onboard system can initiate automatic braking to ensure safety. The communication between the trackside and onboard systems occurs in real time, allowing for dynamic adjustments to train speeds and routes. This standardized approach improves safety by ensuring that trains operate within authorized parameters and respond promptly to changing track conditions or signaling information.

3.2. Cybersecurity standards

The landscape of cybersecurity standards that specifically takes into account the railway sector is rapidly evolving. Acknowledging the growing threat landscape and complexity, the EU Commission directed CENELEC to incorporate the fundamental requirements of EU Directives into a Technical Specification. Collaborating railway and cybersecurity experts have developed the recently published TS 50701, detailing the implementation of cutting-edge cybersecurity protection within a railway environment. CLC/TS 50701 incorporates pertinent safety-related aspects (EN 50126) and draws inspiration from various sources such as IEC 62443-3-3 CSM-RA, customizing them to fit the railway context. The technical specification comprehensively addresses vital subjects, including railway system overview, cybersecurity throughout the railway application life cycle, risk assessment, security design, cybersecurity assurance and system acceptance, vulnerability management, and security patch management. This document was released in 2021. In 2022, the International Electrotechnical Commission began working on railway cybersecurity standard IEC 63452 with the aim of helping rail operators and suppliers fill the gap between physical safety and digital security. The standard aims to map and adapt the requirements of the IEC 62443 series standards to the railway application domain and links the security requirements with the generic reliability, availability, maintainability and safety (RAMS) life cycle of the IEC 62278 series standards. It is expected to be published in 2025.

4. CYBERSECURITY ISSUES

We identify two main communication channels that can be prone to cyberattack, as shown in Figure 2. The first one is the communication between the Balise and the onboard communication systems.

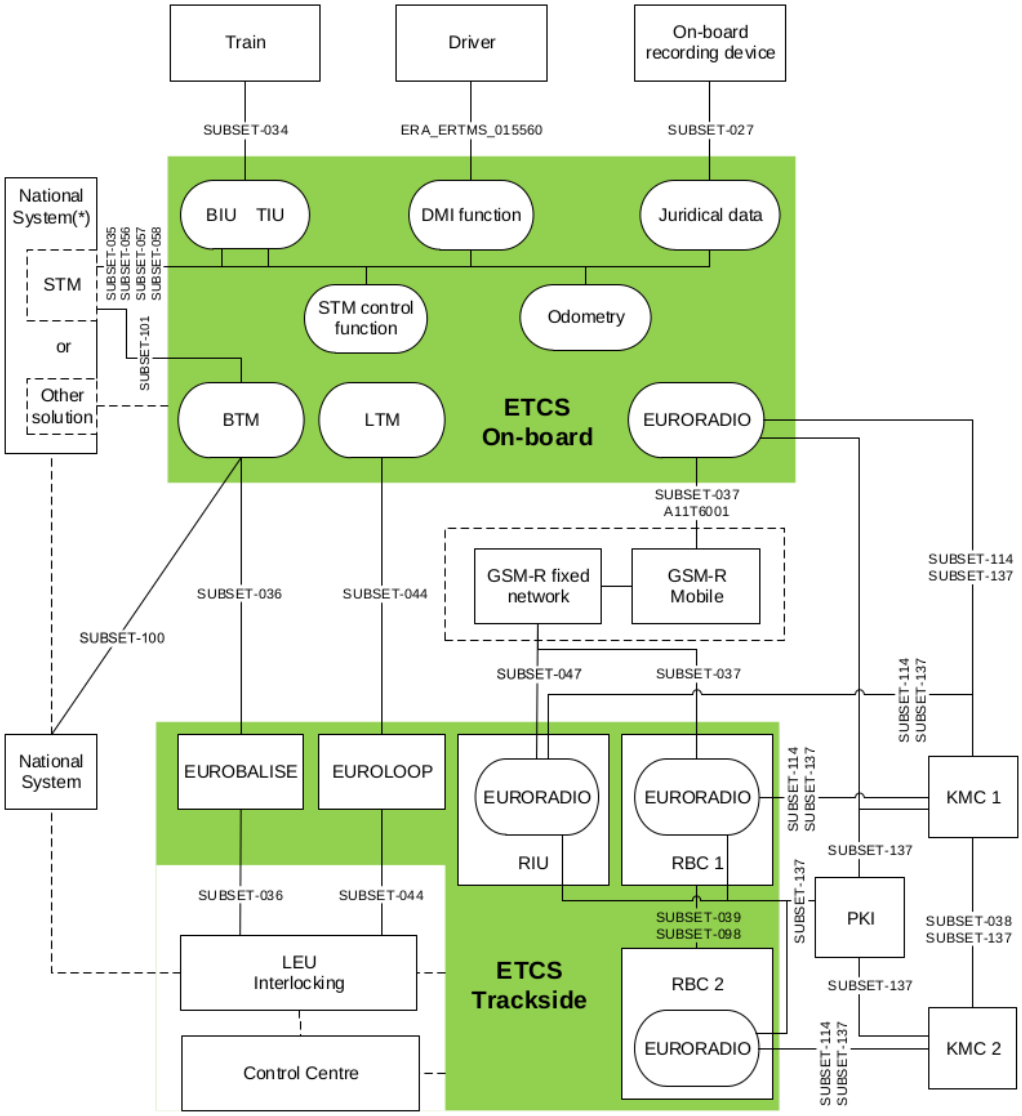

Figure 1. The architectural scheme of ETCS, taken from the standard.

In this case, the attacker has to get close to the devices, which could generally be feasible, since the railways are geographically distributed networks in which it is almost impossible to guarantee physical security. The second case is the long-range communication based on cellular technologies. In this case, the rogue actor can attack the network from a relatively long distance.

One of the main concerns in the railway environment is that many logics are designed based on the principle of intrinsic safety. This means that, in many cases, the absence of communication implies the stopping of vehicles. At the same time, wireless communication is generally prone to denial of service (DoS) attacks, and the protocols commonly used in railways are not particularly robust against this type of attack, as detailed in the next sections.

4.1. Communication between Balises and Onboard Systems

The communication between balises and onboard systems, following the ERTMS standard, forms the backbone of modern rail transportation. Balises, placed along tracks, emit signals that are decoded by onboard

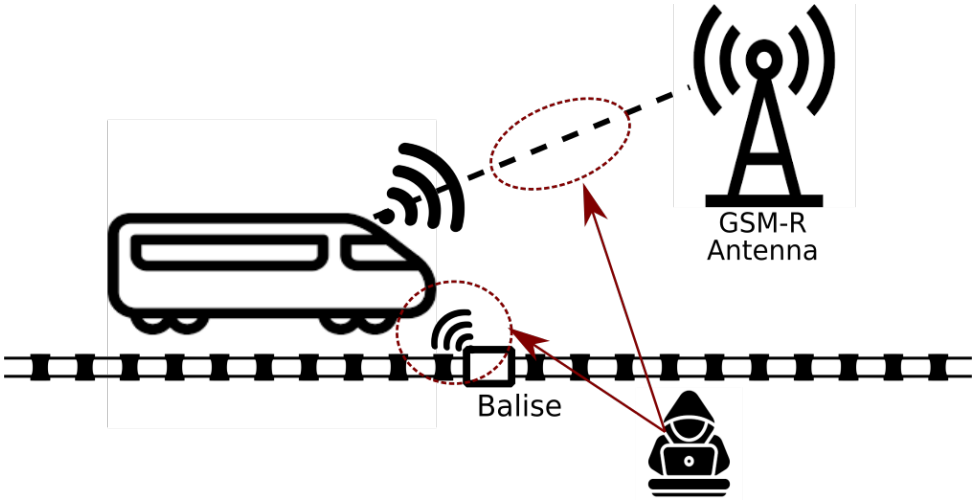

Figure 2. Attack surface.

units. This real-time exchange enables trains to adjust speed and operations swiftly, ensuring safety and efficiency across diverse railway networks. The onboard and trackside equipment in the ERTMS/ETCS system exchange information using the EuroRadio protocol. When an ETCS equipment establishes a connection with another ETCS equipment, both must be able to authenticate the other equipment and verify that it is an authorized entity. The method for authenticating both communicating entities is based on an Identification and Authentication (I&A) dialogue is detailed in [14]. When the ETCS onboard system (BTM) couples with balises, the balises transmit telegrams to the train using the up-link signal. This signal is narrow-band and modulated using Frequency Shift Keying (FSK), exhibiting the following characteristics:

- frequency: 4.234 MHz ± 5 kHz
- telegram coding: BCH
- telegram length: 341/1023 bits
- data-rate: 564.48 kbps

This communication has not been designed to take modern cyber attacks into account. The ERTMS standard does not take jamming into consideration as a security threat that can interrupt the communication between BTM and balises [15]. Temple *et al.* [16] showed how disabling one or more Balises within a metro rail system can significantly impede the train's capability to execute automated stops, potentially jeopardizing the overall safety of the system.

Many balise communication systems lack cryptographic primitives to counter malicious adversaries. Instead, they rely on error correction techniques and mechanical safeguards against external interference. Consequently, a simple attack involves falsifying a balise to transmit arbitrary uplink telegrams. The onboard BTM is unable to filter out these fake telegrams, as they can successfully pass the verification process. Additionally, since fixed balises always transmit unchanging telegrams, adversaries can easily replay these telegrams at various locations to deceive passing trains and control centers [17]. By strategically disrupting wireless signals of balise telegrams, [18] identifies three potential attacks that could lead to passengers falling and causing injuries. Specifically, the first attack involves jamming telegrams in a way that balises cannot be detected by passing trains. The second attack manipulates the location of transmitting telegrams by employing jamming and replay techniques. The third attack involves altering the total time of transmitting telegrams. All these attacks exploit the train localization mechanism, causing passing trains to inaccurately determine their positions and take improper control actions. Additionally, since these attacks operate independently, they can be executed simultaneously to carry out sophisticated assaults.

In practice, denying the communication between the balise and the onboard system is generally feasible with limited resources; the related impact has to be evaluated and, in some cases, can cause cascade effects, which can threaten the availability of large portions of the infrastructure. Moreover, in some implementations, it could be possible to send malicious commands to the onboard system; the related impact can be much higher, causing incidents between vehicles. Also, the ERTMS Security Core Group highlights how most of the implementation of ERTMS may not be secure and would produce a high risk under a risk assessment phase based on the IEC 62443, which is the standard on which the domain-specific standards discussed in Section 3 [19]. While, due to the intrinsic safety mechanism described above, any local attacker can stop a train more easily by physically placing things on the track that make the ETCS believe that there is another train on the rail, the cyber vulnerabilities that can produce DoS remain significant for multiple reasons. For example, causing DoS through a cyber attack instead of a physical manumission can be sneakier, remaining undetected for more time; additionally, it would be possible to activate itself at precise times during the day, even much time after the placement of the rogue device, under the verification of certain conditions; in this way, it could be possible to physically access the railways in times in which the physical security cannot be guaranteed, and then activate the attack later. For these reasons, further work has to be done in this field.

4.2. GSM-R

GSM-R is a telecommunications standard rooted in the ETSI GSM standard. In European regions, GSM-R functions within the 4 MHz frequency range (876–880 MHz and 921–925 MHz for uplink and downlink) and is tailored for radio communications exclusively designed for the railway sector. The ERTMS standard also defines the Euroradio protocol, which allows communication based on an open communication network, such as GSM-R. Euroradio specification is composed of different layers that can be implemented through a stack of different software layers communicating each to the other and commonly make use of the GSM-R. From a cybersecurity perspective, the main criticalities reside right in the GSM-R.

In most of the implementations, the main rule states that a train will automatically halt if the GSM-R mobile terminal onboard detects a loss of connectivity with the Onboard Eurocab architecture. This measure ensures that the train does not proceed on a railway track with incorrect traffic parameters. In case of signal loss, GSM-R base stations promptly alert the network management center. This mechanism is in place to guarantee the safety of both the train and its passengers and cargo. To minimize the risk of service denial caused by jamming attacks and failures of base stations, fixed network components, and radio terminals, the GSM-R network is meticulously designed. Typically, GSM-R base stations are spaced 7 to 15 km apart to offer redundancy, although geographical features and business considerations can influence these distances. Additionally, uplink power control algorithms are implemented for redundancy. However, it is important to note that a powerful jamming attack can overcome these mitigation strategies. Disrupting the GSM-R radio link of even a single train has significant repercussions throughout the railway network, as the movement of each train is interconnected with the positions of other trains in the network [20].

As said, since the protocol is basically derived from the GSM standard, GSM-R has the same well-known weaknesses as the GSM protocol. The GSM presents several issues. ADubey *et al.* [21] demonstrated the vulnerabilities in GSM by using USRP B200 and open-source penetration tools. Chothia *et al.* [22] present an attack that exploits weaknesses of the EuroRadio MAC algorithm used to secure communication between trains and backend equipment; they conclude that EuroRadio is not safe to be used with a transport protocol faster than GSM-R. de Ruiter *et al.* [23] conduct a formal analysis of the communication protocols employed in the ERTMS standard, specifically focusing on the EuroRadio protocol; while their examination reveals that the protocol incorporates a majority of essential security features, it is identified to have vulnerabilities such as undetectable message deletion and the potential for forging emergency messages. The implications of these findings are discussed, and recommendations are proposed to strengthen the overall security of ERTMS. Lopez and Aguado [24], after providing a security evaluation of the European train control management system,

ERTMS, conclude that GSM-R needs replacing, and they provide four main recommendations: a more robust cryptographic mechanism, a new key distribution scheme, a new key storage and system integrity module, and a set of countermeasures for avoiding radio jamming attacks.

Probably the best method to address this issue will be the direct change of the protocols, evolving toward more modern mobile technologies, such as LTE-R[25]. The GSM technology is going to reach its end-of-life status by 2030. The need for a successor to GSM-R is driven primarily by the eventual obsolescence of the underlying GSM technology on which GSM-R is based[26].

The UIC's FRMCS program is planning to take into account "5G"-based technologies (specifically 3GPP R15/16), thereby skipping two technological generations[27]. The future FRMCS mobile radio network in 5G technology to be built along railway lines and the existing GSM-R network will operate in Europe-wide licensed and harmonized frequency bands (900 MHz range and 1,900 MHz range) under the recent European Commission's Implementing Decision (EU) 2021/1730. The standard, however, is still under construction. The FRMCS specifications will be completed with ETSI technical specifications, delivered by the ETSI Railway Telecom technical committee. The tentative roadmap foresees that the market readiness of the standard will be reached in 2026[28]. This suggests that the GMS-R technology will play a role in the railway infrastructure for several years. For this reason, it is necessary to take into account the risks associated with this technology.

5. CONCLUSIONS

This paper analyzed the main vulnerabilities that affect the wireless communication of the ERTMS standard in the railway environment. The shift towards more advanced technologies for mobile communication, such as 5G-based protocols, can significantly enhance the security of communication. Nevertheless, GSM technology will continue to play a crucial role for several years. While security countermeasures are limited to the intrinsic design of the protocol, the risk can be mitigated by following other strategies. For example, cybersecurity monitoring solutions specifically designed for GSM-R can be implemented without substituting any legacy component. At the same time, some aspects of the Onboard-Trackside communication issues can be considered even more serious. While an attack toward this communication requires physical access to the infrastructure, this usually does not represent a big deal for malicious actors due to the impossibility of guaranteeing physical security in such a geographically distributed infrastructure. For these reasons, further work has to be done to enhance the security of these systems.

DECLARATIONS

Authors' contributions

Made substantial contributions to the conception and design of the study and performed data analysis and interpretation: Gaggero GB

Provided administrative, technical, and material support: Girdinio P, Marchese M

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. Teo ZT, Tran BAN, Lakshminarayana S, et al. SecureRails: towards an open simulation platform for analyzing cyber-physical attacks in railways. In: 2016 IEEE Region 10 Conference (TENCON). IEEE; 2016. pp. 95–98. DOI
2. Wang Z, Liu X. Cyber security of railway cyber-physical system (CPS)–a risk management methodology. *Communic Transp Res* 2022;2:100078. DOI
3. López-Aguilar P, Batista E, Martínez-Ballesté A, Solanas A. Information security and privacy in railway transportation: a systematic review. *Sensors* 2022;22:7698. DOI
4. Soderi S, Masti D, Lun YZ. Railway cyber-security in the era of interconnected systems: a survey. *IEEE Trans Intell Transp Syst* 2023. DOI
5. Ai B, Cheng X, Kürner T, et al. Challenges toward wireless communications for high-speed railway. *IEEE Trans Intell Transp Syst* 2014;15:2143–58. DOI
6. Virus Disrupts Train Signals. Available from: https://www.cbsnews.com/news/virus-disrupts-train-signals/ [Last accessed on 21 Feb 2024]
7. Polish teen derails tram after hacking train network. Available from: https://www.theregister.com/2008/01/11/tram_hack/ [Last accessed on 21 Feb 2024]
8. Hackers breached railway network, disrupted service. Available from: https://www.wired.com/2012/01/railyway-hack/ [Last accessed on 21 Feb 2024]
9. BlackEnergy infected also Ukrainian Mining and Railway Systems. Available from: https://securityaffairs.com/44452/hacking/blackenergy-mining-and-railway-systems.html [Last accessed on 21 Feb 2024]
10. Hackers breach Iran rail network, disrupt service. Available from: https://www.bloomberg.com/news/articles/2022-02-27/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia#xj4y7vzkg [Last accessed on 21 Feb 2024]
11. Belarus hackers allegedly disrupted trains to thwart Russia. Available from: https://www.reuters.com/world/middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/ [Last accessed on 21 Feb 2024]
12. The cheap radio hack that disrupted Poland's Railway System. Available from: https://www.wired.com/story/poland-train-radio-stop-attack/ [Last accessed on 21 Feb 2024]
13. European Rail traffic management system (ERTMS). Available from: https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms_en [Last accessed on 21 Feb 2024]
14. On-line Key Management FFFIS. Available from: https://www.era.europa.eu/system/files/2023-01/sos3_index083_-_subset-137_v100.pdf [Last accessed on 21 Feb 2024]
15. Soderi S, Hämäläinen M, Iinatti J. Cybersecurity considerations for communication based train control. https://www.researchgate.net/publication/291332739_Cybersecurity_considerations_for_Communication_Based_Train_Control [Last accessed on 21 Feb 2024]
16. Temple WG, Tran BAN, Chen B, Kalbarczyk Z, Sanders WH. On train automatic stop control using balises: attacks and a software-only countermeasure. In: 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE; 2017. pp. 274–83. DOI
17. Wu Y, Weng J, Tang Z, Li X, Deng RH. Vulnerabilities, attacks, and countermeasures in balise-based train control systems. *IEEE Trans Intell Trans Syst* 2016;18:814–23. DOI
18. Wu Y, Wei Z, Weng J, Deng RH. Position manipulation attacks to balise-based train automatic stop control. *IEEE Trans Veh Technol* 2018;67:5287–301. DOI
19. ENISA-ERA Conference CYBERSECURITY in RAILWAYS. Available from: https://www.era.europa.eu/system/files/2022-12/04CybSecChallenges-2%20-%20ERTMS%20UG%20-%20Cybersecurity%20guidelines%20in%20support%20of%20ERTMS.pdf [Last accessed on 21 Feb 2024]
20. Baldini G, Fovino IN, Masera M, et al. An early warning system for detecting GSM-R wireless interference in the high-speed railway infrastructure. *Int J Crit Infrastruct Prot* 2010;3:140–56. DOI
21. Dubey A, Vohra D, Vachhani K, Rao A. Demonstration of vulnerabilities in GSM security with USRP B200 and open-source penetration tools. In: 2016 22nd Asia-Pacific Conference on Communications (APCC). IEEE; 2016. pp. 496–501. DOI
22. Chothia T, Ordean M, De Ruiter J, Thomas RJ. An attack against message authentication in the ERTMS train to trackside communication protocols. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security; 2017. pp. 743–56. DOI
23. de Ruiter J, Thomas RJ, Chothia T. A formal security analysis of ERTMS train to trackside protocols. In: Reliability, Safety, and Security

of Railway Systems. Modelling, Analysis, Verification, and Certification: First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings 1. Springer; 2016. pp. 53–68. DOI

24. Lopez I, Aguado M. Cyber security analysis of the European train control system. *IEEE Commun Mag* 2015;53:110–16. DOI
25. He R, Ai B, Wang G, et al. High-speed railway communications: From GSM-R to LTE-R. *IEEE Veh Technol Mag* 2016;11:49–58. DOI
26. Pujol F, Marcus JS. Evolution of GSM-R. Available from: https://www.era.europa.eu/system/files/2022-11/Study%20on%20the%20evolution%20of%20GSM-R%20by%20IDATE-WIK_0.pdf [Last accessed on 21 Feb 2024]
27. He R, Ai B, Zhong Z, et al. 5G for railways: next generation railway dedicated communications. *IEEE Commun Mag* 2022;60:130–36. DOI
28. Future railway mobile communication system. Available from: https://uic.org/rail-system/telecoms-signalling/frmcs [Last accessed on 21 Feb 2024]