





Article

Securing the Future Railway System: Technology Forecast, Security Measures, and Research Demands

Simon Unger ^{1,*} , Markus Heinrich ² , Dirk Scheuermann ³ , Stefan Katzenbeisser ^{1,2,*}, Max Schubert ², Leon Hagemann ² and Lukas Iffländer ⁴ 

¹ Chair of Computer Engineering, Faculty of Computer Science and Mathematics, University of Passau, 94032 Passau, Germany

² INCYDE GmbH, 10117 Berlin, Germany; markus.heinrich@incyde.com (M.H.); max.schubert@incyde.com (M.S.); leon.hagemann@incyde.com (L.H.)

³ Fraunhofer SIT, 64295 Darmstadt, Germany; dirk.scheuermann@sit.fraunhofer.de

⁴ Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn Bundesamt, 01219 Dresden, Germany; ifflanderl@dzsf.bund.de

* Correspondence: simon.unger@uni-passau.de (S.U.); stefan.katzenbeisser@uni-passau.de (S.K.)

Abstract: The railway industry—traditionally a conservative industry with low adaption speed for innovation—is currently entering its digitization phase. The sector faces a challenge in integrating new technologies and approaches into the employed—often safety-critical—systems. Keeping the systems secure while conforming to the demanding safety norms creates previously unknown problems. In the last decades, the number of attacks on the railway system has increased. Furthermore, with standardized digital technologies, the attack surface will keep growing. Therefore, in this work, we look into the foreseeable future of the railway system and present 21 likely use cases. We analyze these use cases regarding possible threats, rate the severity of these threats, and deduce and rate necessary countermeasures. To this end, we model these use cases and the corresponding threats and countermeasures using Attack Graphs. We use a graphical solution for the risk and security analysis due to advantages over other methods, i.e., table-based solutions, like simplified presentation and an easier understanding of relationships, dependencies, and interactions between various elements. From these Attack Graphs, we extracted 14 commonly recurring attack strategies. After analyzing 49 countermeasures regarding their current maturity and further research and standardization demands, we identified 21 in need of further investigation. This implies that 21 necessary countermeasures to secure these future use cases require further research to apply to railway systems or require standardization. These results will help researchers focus on the necessary research and standardization and railway operators to ensure the security of their systems.

Keywords: railway system; Attack Graphs; technology forecast; security threats; security measures; standardization; research demand; transportation; critical infrastructure



Citation: Unger, S.; Heinrich, M.; Scheuermann, D.; Katzenbeisser, S.; Schubert, M.; Hagemann, L.; Iffländer, L. Securing the Future Railway System: Technology Forecast, Security Measures, and Research Demands. *Vehicles* **2023**, *5*, 1254–1274. <https://doi.org/10.3390/vehicles5040069>

Academic Editor: Pedro Antunes, Hugo Magalhães, Pedro Aires Montenegro

Received: 27 July 2023

Revised: 30 August 2023

Accepted: 19 September 2023

Published: 25 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Future railway networks are expected to provide more capacity. For example, in Germany, the goal is to provide up to one-third more [1]. Since 2019, the German government has increased its annual investment in Germany's primary railway infrastructure operator, Deutsche Bahn's rail network, to realize this goal. Surpassing road infrastructure funding for the first time in 2022. The German government aims to double passenger numbers by 2030, primarily for climate policy reasons [2].

Significant performance improvements are necessary to achieve these objectives. This pertains to every aspect of the entire railway system, starting from traffic control and the utilization of the existing rail network to managing passenger flows at stations and aboard vehicles, facilitating a seamless connection to various transportation modes for the smooth and controlled movements of goods and passengers. Consequently, a comprehensive

digitization of the technology and operational processes of the railway system is required. This objective not only fosters new technological trends but also enhances the capacity and attractiveness of the overall railway system. However, it also introduces new security vulnerabilities and risks, posing threats to the availability and operational safety of the railway system.

An analysis of physical attacks on the railway system by Iffländer et al. [3] shows that attacks have been drastically rising since the 1990s. Moreover, 35 out of the 127 attacks that have been analyzed have taken place in the last decade. This shows that the railway system is an increasingly popular target. Likely due to its high vulnerability and wide-spread and easily accessible network, it can be declared a so-called “soft target” [4].

In the “Forecast of security requirements and evaluation of possible security concepts for the railway system” project, we addressed the tension between technological trends and the challenges of threats by investigating the following research questions: (1) What technologies will be used in railway systems up until 2050? (2) What are the use cases for these technologies? (3) What threats are posed by these technologies and use cases? (4) How can we secure the systems against such threats? (5) Have the countermeasures to protect the systems against threats been researched enough and standardized for use in railway systems? To answer these questions, we began with a technology forecast up to 2050, describing use cases for a comprehensive overview of new technology. Using the technology forecast, we identified use cases covering all railway subfields, ranging from passenger and freight transport, over rolling stock and infrastructure, to train protection and signaling technology, as well as railway operations, traffic management, and maintenance. The use cases establish the connections between technologies, data flows, and benefits, directly utilized to identify security needs. To identify the threat landscape, we developed a methodology of Attack Graphs and derived an Attack Graph for every use case. After the identification of the threat landscape, we identified countermeasures necessary to secure the use cases. These countermeasures were then analyzed regarding their current technical states to identify those that required further research and standardization.

Using the technology forecast, we identified 21 use cases describing the used technologies and their relations. For each use case, we constructed Attack Graphs to depict the threat landscape, unearthing 14 recurring attack strategies that threaten these use cases. To secure future systems against those attacks, we identified 49 countermeasures; 28 of them are already established solutions ready for deployment in railway systems and are mandated by standards for implementation. That leaves 21 countermeasures grouped into 6 categories that are not sufficiently developed to be used in railway systems and/or are not mandated by standards for deployment.

Defining Attack Graphs as a graphical solution for the risk and security analysis mitigates the disadvantages of other risk and security analysis solutions, i.e., table-based solutions. The first advantage of Attack Graphs is that a visual representation of the security landscape enhances the understanding and communication of complex risk information and simplifies the identification of patterns, trends, and relationships among threats and risks. Furthermore, different risk scenarios can easily be explored by manipulating variables or parameters or adapting different countermeasures within the visual representation, enabling the assessment of the potential impacts of various risk factors and the evaluation of the effectiveness of different response strategies.

The remainder of the paper is structured as follows: After the introduction, Section 2 briefly introduces the related work to our goals. All derived use cases are described in Section 3. The developed methodology of Attack Graphs to support the risk analysis is summarized in Section 4. In Section 5, we identify frequently recurring attack strategies and countermeasures that still require research and standardization. Finally, Section 6 presents an outlook on the further work needed to evolve the derived countermeasures.

2. Related Work

To the best of our knowledge, no study exists that answers all of our research questions. However, there are studies that help to answer research questions 1 and 2; the most relevant are presented below.

It is necessary to know the threats to these future systems to identify the research and standardization demands of security measures for the future railway system. Furthermore, it is necessary to know the technologies used in future railway systems to identify the threats. As the railway system takes up innovation rather slowly, especially technologies that impact safety, some future technologies are already known, as they are being researched and developed. These technologies can be found in the literature and roadmaps of railway operators, federal offices, and research publications. These technologies include automatic train operation (ATO) [5,6], communication-based train control (CBTC), digital interlocking, the Future Railway Mobile Communication System (FRMCS), infrastructure modeling [7], the European Train Control System (ETCS) [8], train-to-train communication [9], predictive maintenance, global navigation satellite system (GNSS), innovative train integrity systems, fiber optic sensing, industrial robots, robotic assistants [10,11], and intelligent automation.

Furthermore, a report by Arup Rail titled “Future of Rail 2050” [12] describes how they envision the railway system up until 2050 and the technologies they deem necessary. Some of their envisioned technologies have security impacts, making them essential to our research. These include autonomous trains, real-time passenger information, intelligent robots, and drones. However, the study does not include specifics about technologies, and more notably, it omits insights on security issues, countermeasures, and the urgency for research and standardization. To further identify technologies and use cases, we looked into industries like the automotive industry.

To identify threats, multiple publications exist on specific technologies, which can further be adapted or envisioned for the railway industry. For example, Iffländer et al. covered physical attacks on the railway system that occurred in the past [3]. They analyzed physical attacks on railway systems worldwide and collected 127 events since the late 1800s. The attacks were structured and evaluated according to types of attackers, means of attack, targets of the attacks, and incurred damage. Their analysis indicates a significant rise in attacks and casualties since the 1990s. Furthermore, the means of attack are becoming more diverse. This study supports the security analysis regarding possible physical threats. However, it does not include digital attacks, security countermeasures, their state of research, or standardization.

3. Technology Forecast

The project team oversaw the development of the technology forecast. To expand the technology forecast predictions across the future railway system, the expansive expertise of the project partners in the railway and automotive sectors was extended by members from the areas of industry, research, and operational backgrounds to form a team of experts.

The determination of security requirements for the future railway system is based on a technology forecast that anticipates the digital technologies that will be utilized in the next 30 years as use cases.

Our technology forecast involved a three-stage process:

- Literature research and discussions within the project team.
- Workshops with an expert team stemming from railway operators, railway manufacturers, and academia.
- An exchange between the project and expert teams.

In stage 1, the existing specialist knowledge from the literature was documented, including the expectations of the project members. In stage 2, semi-structured workshops were held with the expert team, with the goal of

1. Finding features of the railway system that fall into the categories shown in Figure 1; and

- Identifying future technologies that will be available until 2050 and could be integrated into the railway system.

For the technology forecast, 21 use cases (summarized in Section 3.3) were defined across 6 areas: passenger and freight traffic, train protection and signaling technology, rolling stock, trackside infrastructure, as well as railway operation, traffic management (dispatching), and maintenance; they describe the application of digital technologies in future scenarios (see Figure 1).

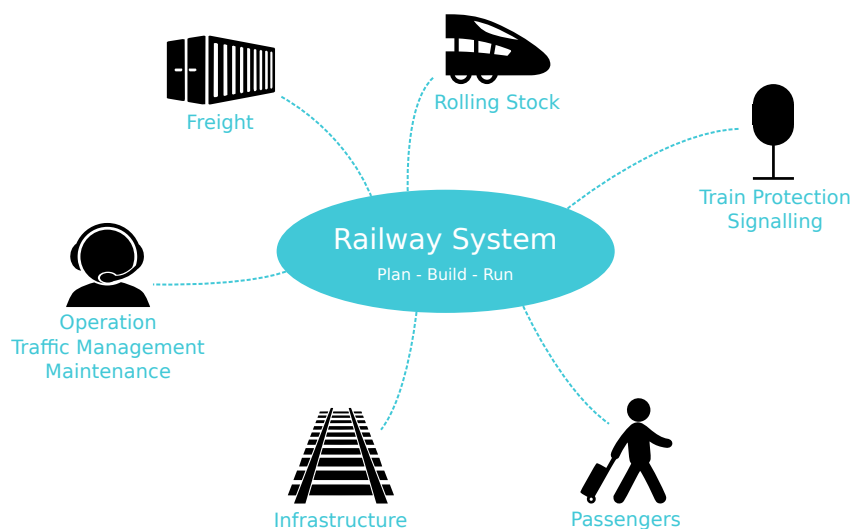


Figure 1. Areas of the railway system considered in the technology forecast.

While creating the technology forecast, two fundamental goals were pursued: sufficient completeness of the technology forecast and mutual validation.

3.1. Goal 1: Sufficient Completeness

Absolute completeness is challenging to achieve, with a forecast extending up to the year 2050. This particularly applies to the railway system that has numerous subsystems. The heterogeneity of the different subsystems caters to various technologies and use cases. The expert team members take interdisciplinary perspectives on the railway system and, thus, round off the technology forecast to obtain a complete picture. By consulting experts without a specific focus on the railway system, who are unaffected by the limits of the existing system, there is an opportunity to capture innovation that may remain hidden from internal experts. In addition, the technology forecast aims to assess the need for future IT security mechanisms, not to craft a perfectly accurate depiction of the railway or transport sector. Under these conditions, a certain amount of uncertainty in the technology forecast was deemed acceptable. Drawing knowledge from the literature and the expert team ensured sufficient completeness of our technology forecast.

3.2. Goal 2: Mutual Validation

The technological trends and expectations formulated by the expert team were utilized, among other purposes, for the validation of the technology forecast. To keep the mutual influence low, the expert team was divided into two groups to perform the workshops. Both groups independently mentioned the same or similar technologies and scenarios, thus validating each other and pointing to a reliable forecast. Accordingly, as expected, there were overlaps in the forecast technologies and use cases.

3.3. Use Cases

In this section, we briefly describe the 21 derived use cases. A detailed description of the derivation process and all the use cases can be found in Leining et al. (in German) [13]. The use cases we designed describe the employment of future technologies and their

interactions. Therefore, we do not provide detailed architecture. Also, specific architectures can be different depending on the company or operator. However, for our research, this level of detail was not necessary. Understanding the technologies used and their communication medium is enough to identify the threats to the system. It is not necessary to know, e.g., how many routers are in the network. A single one might be enough for the system to be vulnerable, and multiple routers might only increase the attack surface.

Automated hump control. In marshalling yards, automated processes are used to assemble trains by shunting wagons. An automatic shunting locomotive pushes the coupled train over the hump, and the separation of wagons is achieved through the use of digital automatic coupling (DAC) on different destination tracks. To enable this, wagons must be equipped with digitally readable identifiers for detection along the track.

Automated planning and plan review. Planning processes today rely on subjective interpretations of rules written in prose, which can lead to inconsistencies. A complete and logical mapping of the planning rules using mathematical relations and logical connections enables the identification of the best and formally correct solutions while detecting conflicts with defined goals. The same automated process can be applied to plan reviews, using different logical connections to ensure independence and prevent logical shortcuts.

Cloud interlocking. The trend of centralizing interlocking systems continues towards centralized cloud-based solutions, offering infrastructure companies the ability to control their entire network from a single data center. This cloud-based interlocking system is a service, making it an attractive option for smaller networks reluctant to invest in their technology and expertise for a few interlocking systems. To ensure safety, it requires a safe platform and secure communication technologies between the data center and field elements. The advantages include centralized maintenance, backup resource availability, standard components, such as (commercial off-the-shelf (COTS)), and centralized personnel deployment.

Decentralized interlocking. Traditional interlocking systems for track safety are replaced with decentralized methods, where vehicles directly reserve routes or coordinate with each other through V2I or V2V communication. This eliminates the need for conventional interlocking systems. Accurate positioning of trains and infrastructure elements is ensured using technologies like GNSS, enabling secure localization and route planning stored on digital maps.

Emotion and intent recognition. Cameras are used to record the body language of individuals. Afterward, affective computing [14,15] can deduce emotions and intentions using facial expressions, postures, gestures, and, if available, language. This allows one to make conclusions about the passenger's mood or emotional state or it can be used to detect indicators of aggression or willingness to engage in violence early on, allowing for appropriate prevention and de-escalation measures to be implemented.

Remote-controlled rolling stock. Vehicles that can be controlled remotely from a central operation center depend on reliable wireless communication, such as FRMCS, along all possible routes to transmit extensive sensor data to the operations center and control data to the vehicle. Centralized remote control mitigates issues related to driver fatigue as driver relief can be handled more efficiently from a central location rather than dispersed along the route.

Freight route management. In the future, railway operators can offer a service encompassing end-to-end logistics support by integrating various transportation modes. This enables prioritization of low-emission transport routes and optimization of the route based on factors such as the required arrival time, temperature control, criticality for avoiding delays (e.g., just-in-time requirements), optimization of available capacities, and more. This requires a comprehensive digital representation of traffic and customer processes.

Predictive maintenance. Predictive maintenance aims to predict when a failure is likely to occur by analyzing the real-time operational data of the equipment. Predictive maintenance could be further enhanced to eliminate regular maintenance intervals and instead

focus solely on addressing potential failures before they occur through timely maintenance interventions.

Intermodal freight handling. Intermodal freight handling describes the integration of different modes of transportation for efficient goods delivery. Beyond the virtual coupling of trains, individual wagons with their propulsion could be utilized for transporting standardized containers, which can operate on both road and rail or other track-bound systems, like the Hyperloop. The wagons are combined into larger units, utilizing platooning or virtual coupling to cover longer distances and optimize infrastructure utilization. Additionally, the possibility of transitioning to air transport is considered, and the control and coordination of these operations are explored through concepts like “driverless operations” or “cloud-based control”.

Intermodal travel chain. Future mobility will be a service-oriented experience that combines multiple modes of transportation into a seamless journey with shared data and integrated payment systems. This intermodal approach allows travelers to book and pay for their entire trip simultaneously. Advanced technologies, such as biometrics, GNSSs, and short-range wireless communication, enable contactless ticketing, registering the entering and leaving actions of passengers, and automating luggage transfer between different transportation modes.

Contactless ticket control. The ability for passengers to validate their tickets on their smartphones, which is already available today, will be further developed to enable contactless authorization without any interaction with train staff. Upon boarding the train, the digital ticket will be recognized, employing technologies like Bluetooth, NFC, or satellite-based tracking. This process eliminates the need for manual ticket inspections and requires ticket data to be matched with a central authority through communication means like FRMCS or satellite communication.

Optimized travel and price arrangements. Travelers require access to digital platforms that provide comprehensive information on available travel options, pricing, and services, while also accommodating their specific preferences and offering real-time updates on disruptions and alternative routes. These platforms need to integrate data from various travel providers, connect with operational centers and vehicles, and leverage Big Data techniques to handle the complexity and volume of information. By accepting pre-defined travel profiles as input, the platforms can offer personalized recommendations and immediate alternatives to enhance the overall travel experience.

Optimization of passenger changeover time. Sensor-equipped trains monitor the occupancies of different sections and transmit the data to the next station. The data are then displayed to waiting passengers, allowing them to position themselves in less crowded areas before the train arrives. This reduces conflicts between boarding and exiting passengers while improving overall comfort by maximizing available space and minimizing travel distances within the train.

Identification of persons. Identifying individuals has multiple benefits, including analyzing their behavior and providing personalized offers. It also aids in tracking individuals involved in criminal activities or those who are helpless or missing, allowing for targeted responses and the involvement of relevant authorities.

Travel and life management. In the future, railway operators can offer a service for end-to-end customer guidance through a connected multi-modal transportation system. This allows for a preference for public transportation while optimizing schedules and capacities to reduce the drawbacks of rigid timetables. Last-mile options like car sharing, autonomous taxis, and bicycles complement the offering. The foundation is a comprehensive digital representation of traffic and customers, enabling the calculation of an optimal route based on individual requirements, habits, and preferences.

Passenger guidance through the train station. Passengers on the platform should receive real-time information on their mobile devices to minimize infrastructure and provide convenience. Location-based services enable tailored information specific to the platform, utilizing the Internet of Things (IoT), mobile networks, wireless technologies (e.g., LoRa[®])

for longer distances, and shorter-range options (e.g., Bluetooth or ZigBee) for local communication. This approach improves accessibility and ensures passengers remain informed without relying on physical display boards.

Steering action for scheduling. The control center's dispatch utilizes standardized interfaces for immediate operational interventions and relies on a digital twin of the railway system to generate precise forecasts. High computing power from technologies like quantum computers or exascale computing enables real-time optimization and the ability to respond dynamically to transportation demands. The proposed measures are promptly communicated as speed profiles and training paths to vehicles, interlocking, and Radio Block Centres (RBCs) for rapid implementation.

Virtual Coupling. For freight and passenger transportation, transportation units often use shared methods before eventually parting in different directions, or different transportation units from different methods come together. The process of physical coupling and decoupling is time-consuming. The concept of virtual coupling involves avoiding mechanical coupling processes. Instead, automatic steering directs the transport units along predefined routes (together); they are coupled and decoupled to and from different ways at predefined positions.

Fully automated driving. In the future, train journeys will be fully automated, with vehicles performing the operations. Communication with the track infrastructure is essential to avoid conflicts in occupancy and prevent accidents. The vehicle automatically travels along the track to its destination, considering vehicle and track limitations within a speed profile.

On-site information. Upon arrival at the track, passengers need to be supplied with current information, e.g., regarding a sequence of wagons, delays, or track changes. Passengers can obtain information using their mobile devices and contact service applications to navigate to the next sign panel.

ETCS Train Protection. From today's perspective, implementing already standardized ETCS L3, Hybrid L3, and L2oS will significantly influence the train's control system, moving away from traditional track vacancy detection systems. The positioning and train integrity determination are performed continuously on the vehicle side and transmitted to the interlocking or RBC. Train spacing will transition from the fixed block to the moving block, with movement authorizations relayed from the interlocking/RBC to the vehicles.

4. Attack Graphs

In the next step, we conduct a security risk analysis of the developed use cases. To support the risk analysis, we developed the methodology of Attack Graphs and built a software tool to automate the calculations. The underlying methodology and the software tool have been described in more detail by Unger et al. [16] and Heinrich and Iffländer [17]. In principle, the tool allows adapting attributes freely to the current practice of the domain under consideration, existing standards, and the risk affinity of the analyzing organization. The German pre-standard DIN VDE V 0831-104 [18] uses the attributes "resources" and "knowledge" known from the IEC 62443 [19] series and replaces motivation with three railway-specific risk factors, of which, we use "location" for our analysis. This leads to the attribute vectors (resources, knowledge, location).

Here, we only introduce the fundamental concepts and focus on the choices made within the Attack Graph methodology to apply them to our analysis. The tool reduces the amount of work and the susceptibility to errors, increases the traceability and meaningfulness of the analysis, and is freely available as open-source software (<https://github.com/INCYDE-GmbH/drawio-plugin-attackgraphs> Accessed on 22 September 2023).

An Attack Graph specifically analyzes one use case (see Section 3.3) at a sufficiently specific level of abstraction. For our study, we created 21 Attack Graphs accordingly. One graph depicts the analyzed asset by a trapezoid (see Figure 2). Attacks on the asset lead to various consequences or damage events, which are represented in the graph by rectangles with rounded corners. We consider the following consequences in our analysis:

- Financial damage to the operator, an individual, or a customer;
- Reputation damage to the operator, manufacturer, or an individual;
- Violation of laws and regulations;
- Violation of privacy;
- Infringement of property;
- Restriction of a critical service;
- Provoke chaos;
- Market manipulation;
- Obstruction of justice;
- Violation of physical integrity.

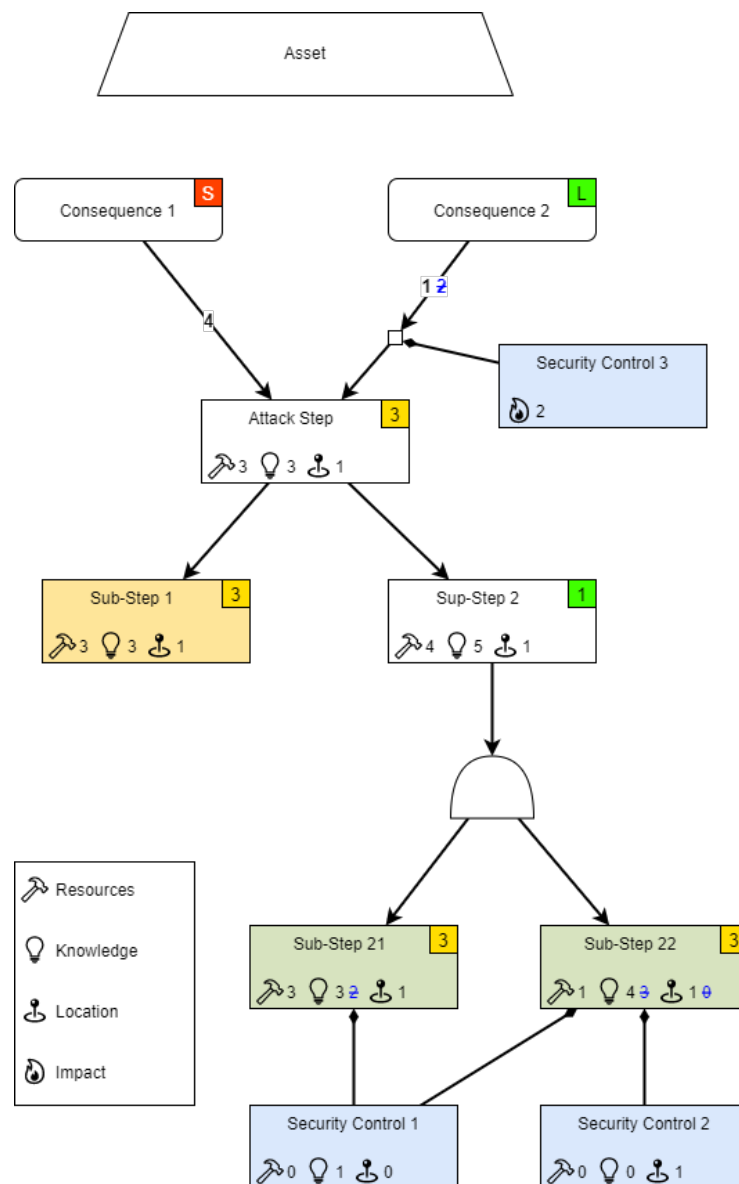


Figure 2. Example of an Attack Graph.

4.1. Refinement of Attacks

Damage events are further refined by considering particular attacks. Each damage event can be triggered by one or more attacks (“attack step” in Figure 2). The graph shows this relationship via a directed edge from the consequence to the attack step. By visualizing this link, the Attack Graphs increase the traceability of the risk analysis since they can graphically represent possible n:m relationships between attacks and con-

sequences. The Attack Graphs support the analysis by graphically breaking down the attacks into sub-steps (“Sub-step 1” and “Sub-step 2” in Figure 2) to refine the analysis and the subsequent risk assessment. Sub-steps may be combined into attacks using logical disjunctions (or) and conjunctions (and). The methodology allows for nested logical operators and is open for extension with other logical operators (e.g., XOR). A directed edge between the nodes represents a division of a step into the sub-steps. Corresponding nodes between two attack steps represent disjunctions and conjunctions (e.g., the AND gate in Figure 2). A direct connection between two attack steps implicitly represents a disjunction. The breakdown of the attack continues iteratively until reaching attack steps whose probability of occurrence (resources, knowledge, and location) can be estimated with sufficient precision.

4.2. Risk Assessment

After setting up the Attack Graphs, the risk assessment process follows a bottom-up approach, starting with the leaf nodes and aggregating results upward to compute the final assessment. In this analysis, the tool evaluates the leaf nodes of the Attack Graphs by a selected vector of attributes to model the probability of occurrence. As described before, we use the attribute vectors (resources, knowledge, location) taken from the German pre-standard DIN VDE V 0831-104 [18], which is based on the IEC 62443 [19] series. The tool visualizes the attributes with the help of icons (see Figure 2). The added value of Attack Graphs comes from atomic leaf nodes, as their attribute assessments are more straightforward than more complex compound attacks. However, this means that it is necessary to aggregate the leaf node evaluations along the path to the damage event to reassemble the sub-steps into an overall assessment. The software tool used for creating Attack Graphs supported analysts through the prepared and automated linking of the sub-steps according to the logical operators defined in the breakdown. A detailed description of the required functions is presented by Unger et al. [16]. A disjunction of attack steps assumes that the attacker chooses the most easily executable step out of several possible sub-steps to implement an attack step. A mathematical order relation over the attribute vectors allows comparing the feasibility of the partial steps and determining the highest feasibility as a scalar from the attribute vector (R, K, L), as depicted in the top right corner of each attack step. For example, in Figure 2, the evaluation of “Sub-step 1” carries over to the “attack step” because it has higher feasibility compared to “Sub-step 2”. The combination of several sub-steps leads to the more complex (and lower) feasibility of the resulting step. The resources and knowledge required for a successful attack have increased, as shown in Figure 2. For illustration, the interposed “AND” node adds the attributes of the child node “Sub-step 21”. The software tool aggregates the attribute vectors automatically toward the parent attack step (against the direction of the edges). Experts also evaluate the impact of an attack or its influence on a specific consequence at the transition from the attack step to the consequence. The estimated impact is represented as the edge weight of the edge between the attack step and the consequence. An aggregation function in the consequence node accepts each child node’s attribute vector and the impact (edge weight). It uses a risk matrix to determine the attack with the highest risk for the damage described in the node (the letter in the top right corner of consequences). The values shown in the figures are for illustration purposes and do not reflect a specific use case.

4.3. Countermeasures

The risk analysis and assessment of the threats can consider countermeasures, which also reduce the risk. Here, we assume an n:m relationship between the attack and countermeasure since, typically, a single countermeasure can protect against several attacks and, conversely, multiple countermeasures can protect against the same attack, or only the combination of several measures can provide adequate protection. Figure 2 shows the effects of two countermeasures on two attack steps and their impacts. The countermeasure evaluation uses the same attribute vectors as attack steps to determine the levels of

mitigation they provide to an attack or impact. The tool displays the original assessment in blue and crossed-out font, while the values printed in black account for the influence of the countermeasures and, thus, reflect the risk reduced by the measure. Both “Security Control 1” and “Security Control 2” reduce the attack feasibility of “Attack Step 1” with the added effect in the example, which eventually leads to a risk reduction. On the other hand, only “Security Control 2” acts on “Attack Step 2”, so there is a minor reduction in feasibility with the same initial evaluation as “Attack Step 1”. “Security Control 3” mitigates the impact of “Attack Step” on “Consequence 2”.

4.4. Outcome

All 21 analyzed Attack Graphs, including the attack paths, the attribute assessment, and the countermeasures, are available online (<https://github.com/INCYDE-GmbH/attackgraphs> accessed on 22 September 2023). In workshops, security experts evaluated attributes for each attack step.

The greater goal of our analysis was to identify future standardization and research demands, i.e., gaps in current technology and requirements in the protection against the anticipated threats that we describe in Section 5.1. We strived for completeness in identifying the gaps in the countermeasures. Still, we did not provide a complete enumeration of measures to reduce the risk of each threat below an acceptable threshold (“low”, in our case). The latter would require demonstrating the completeness of the application of existing countermeasures, which is not necessary to achieve the goal of our analysis.

5. Results and Discussion

Based on the use cases described in Section 3.3 and the resulting Attack Graphs, we identified threats to the future railway system. Analyzing the threats, we discovered that all threats correspond to 14 different categories described in Section 5.1. In order to mitigate these threats, we further identified countermeasures, particularly those that induced research and standardization demands (see Section 5.2).

5.1. Upcoming Threats to the Future Railway System, Inducing Research Demands

After analyzing the 21 generated Attack Graphs, including the identified threats, we grouped them into the following 14 categories.

Unauthorized data access. Unauthorized access to data storage or other components in the railway system poses a threat to large and small datasets, such as configuration or control data, which are crucial for automated railway operations. Manipulating data through unauthorized access to system components and interfaces can entail significant risks, even if only a few small datasets are affected.

Interception of data. Even without manipulation, the interception of confidential data poses a significant threat that can carry high risks. In the context of railways, this primarily concerns passenger data, such as travel profiles or other personally identifiable information (PII). Unauthorized interception of such data during the use of services, like passenger guidance or travel management, represents a violation of the passenger’s privacy. An analysis of the use cases indicates that as there is a rise in individualized, profile-based assistance for passengers coupled with data protection regulations, new risks arise that require adequate concepts to protect privacy (ideally “Privacy by Design”).

Tampering with Wireless Transmission. In the future, communications in railway systems will increasingly rely on wireless technologies, such as mobile networks, satellite communication, or short-range technologies, like Bluetooth or Sigfox. Wireless communication plays a significant role, especially in machine-to-machine (M2M) communication and, therefore, it needs to be protected. However, remote-controlled vehicles are also attractive targets that will be used, for example, for shunting operations or in ATO systems. Attack scenarios include disrupting wireless communication, such as blocking M2M transmissions or preventing remote control. Furthermore, false data packets can be injected, leading to incorrect

occupancy or the release of tracks in M2M communication, or in the case of remote control, taking control of the vehicles.

Attacks by quantum computers. Quantum computers utilize qubits instead of classical bits, allowing for coherent superposition of the 0 and 1 states. This provides an advantage in computational speed over classical computers, enabling exponentially complex calculations to be performed much faster. However, quantum computers do not pose a significant threat at present because they still have very few qubits. Many techniques for ensuring integrity and authenticity rely on calculations that become exponentially more difficult as the bit length increases. Nevertheless, research institutions and industries are continuously working toward expanding and improving their quantum technologies, which may pose a future threat to security. Therefore, it is essential to use methods that ensure integrity and authenticity, which are robust enough to counter potential threats from quantum computers.

Manipulation of (large) databases. As railway operators seek to improve their systems, expand their offerings, and provide personalized services, data collection becomes increasingly essential. The data are necessary for various applications, such as enabling predictive maintenance, training artificial intelligence (AI) models, and offering tailored products to individual customers. Therefore, the storage of large datasets plays a crucial role. It is vital to ensure the data are neither lost nor compromised in integrity. Failure to renew system components appropriately by predictive maintenance can lead to financial or, in the worst case, personal harm. Manipulating training data for AI systems can also compromise the intended function of the AI. Customer-related data pose significant risks, especially in future use cases like intermodal travel, where sharing data with other transportation service providers may be necessary to a certain extent. However, even in more conventional applications, such as contactless ticket inspection and passenger identification, it is crucial to ensure the privacy of individuals. Paradoxically, the provision of anonymized data can still threaten individual privacy since, with an increasing amount of available data, it is possible to identify individuals through data correlation, even if all the data are anonymized. Therefore, it is essential to ensure the confidentiality, integrity, and authenticity of datasets.

Attacks on the digital capture of the environment. Like many other industries, the railway sector relies on an ever-increasing amount of digital data of various types. Even without attackers, creating and maintaining an accurate digital representation of the analog world is already a challenge. This challenge is further amplified by the use of digital twins, which monitor the digitally cloned system in near real-time for changes (such as the movement of trains or people and reactions to environmental conditions). Through cyberattacks, the dimensions of deliberate and concealed manipulations of the real-time digital representations of the analog world come into play. Attackers could manipulate infrastructure data in digital maps (used, e.g., by ATO) to provoke accidents or disrupt railway operations on a large scale. For example, suppose measurement data from autonomous trains are manipulated and do not accurately reflect reality. In that case, they can impact functional safety and potentially enable extortion of the operator. Applications such as automated or autonomous driving heavily rely on the accurate perception of the environment. A future challenge will be to ensure high trust in the correct collection and retention of different datasets. Technical approaches to address this challenge may include validation through historical data points or integrating different measurements.

Manipulation of machine-to-machine communication. As the railway system undergoes digitization, the technology forecast also predicts the automation of various processes. This leads to an increase in communication between system components, such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and other forms of M2M communication. It opens up new targets for attackers since actions previously carried out mechanically can now be triggered digitally. One potential risk exists in opening a DAC to stimulate train separation, which could, in the worst case, pose a safety hazard to following trains. Regarding decentralized interlocking and driverless operations, M2M communication plays a significant role. It can be abused to disrupt or transmit false track occupancy

between infrastructure, vehicles, and control centers. Moreover, components not originally part of the system (the attacker's devices) can be introduced to execute these attacks. Therefore, this communication must be protected against manipulation by ensuring the authenticity of communication partners and the integrity of messages.

Attacks on Machine Learning. Predictive maintenance is the most prominent example of using machine learning (ML) in the identified scenarios. ML and AI are also employed in other scenarios to fulfill partially critical functions. A threat arises from the fact that decisions are increasingly entrusted to AI, but such decisions are not equally as transparent and traceable as those made by humans. Attackers can exploit this situation to manipulate decisions in their favor. Relying entirely on predictive maintenance, e.g., by eliminating regular maintenance intervals for points, can lead to point failures. Obstacle detection based on the AI-based analysis of camera images can be deceived by existing obstacles to provoke collision. Such attacks can be carried out by manipulating the AI model if its integrity is not adequately protected.

Adversarial machine learning [20] has shown that ML can be deceived in classification through cleverly manipulated inputs. In such scenarios, the attacker leverages knowledge about the algorithm and model to orchestrate an attack. In image recognition, in particular, the manipulations are so subtle that a human observer cannot detect them.

Physical attacks. Currently, providing physical protection against cyberattacks on railway system components is particularly challenging because rail transportation inherently has openly accessible critical components. These include field elements of signaling technology and vehicles with passenger Wi-Fi. The physical attack surface will further expand as monitoring elements become more centralized. For example, the automation of shunting and train operations, as well as remote-controlled train driving, reduce the presence of the train driver, making it more challenging to detect physical manipulation. Signaling technology, in particular, is characterized by a physical separation between functional safety and IT security, which complicates the implementation of a comprehensive defense strategy.

Cyber extortion. Currently, infestation with ransomware and the associated demand for ransom and protection money are dominant patterns of cyberattacks. The analysis of the Attack Graphs indicates that there will be an increased vulnerability of railway system operators in the future, where besides ransomware, other extortion scenarios may also be possible, such as extortion for protection money under the threat of otherwise conducted cyberattacks. This affects both the operational components (signaling technology, dispatching) and the customer relationship (passenger and freight transport). Adequate IT security concepts must be implemented to counter all cyberattacks associated with extortion in the future. The vulnerability to cyberattacks and the threat of cyberattacks result from the increasing automation of processes and the use of digital datasets concerning the infrastructure and the customers. The more crucial a process or dataset is for the availability of critical rail transport services, the more strongly the cyber extortion affects it, as the pressure on the operator is heightened.

Malware. Introducing malicious software into the railway system can cause significant damage in various ways. The use of ransomware followed by extortion is just one example. Other types of malware can directly cause malfunctioning components in the railway system, posing high risks of damage. This includes generating false information about the system's state or manipulating users into engaging in harmful interactions.

Manipulation of safe localization. A variety of processes within the railway system already benefit from location information. These include, for example, the self-localization of customers using the operator's travel app or initial applications in railway operations through driving recommendations transmitted to the train driver on a separate mobile device. In the future, additional services are expected to be introduced that will facilitate dispatching in both passenger and freight transport and provide customers with real-time tracking of their goods. Additionally, safety-related applications such as train positioning and train integrity are intended to be added to reduce the equipment required for the infrastructure. All these applications rely on a purely radio-based positioning system, col-

lectively referred to as GNSS. However, all radio-based services, including GNSS, have the shared vulnerability of being susceptible to jamming. When jamming occurs, the location information becomes unavailable. Processes entirely reliant on GNSS positioning are no longer operational during such incidents. Jamming attacks on GNSS can be relatively quickly executed due to the relatively weak signals from satellites. A more challenging and critical security concern is the spoofing of location information. Spoofing involves falsifying the location information reporting a different location than the actual position, such as a different track or section. In safety-critical applications, this can have catastrophic consequences. Current railway systems, such as locomotives, lack sufficient measures against jamming and spoofing. With the future intensive use of localization methods on vehicles, it is essential to employ methods for protection, detection, and response to jamming or spoofing of localization. Therefore, a resilient architecture implementing these functions is crucial for maintaining safe and available railway operations. The examination of these measures and their expansion to less critical applications must follow to ensure the availability and resilience of convenience-enhancing services against attacks.

Denial-of-service attacks. Jamming, described next, belongs to the class of denial-of-service (DoS) attacks, where the availability of components in the railway system is disrupted. These attack scenarios are not limited to the disruption of radio signals alone. Numerous other attack methods can achieve a DOS. Examples include flooding servers with service requests or mechanically disrupting data transmission by damaging transmission paths.

Jamming. The technology forecast predicts a continued increase in wireless communication systems used in various applications. Functions such as train operation, safety, passenger information, freight transport, and intermodality rely on wireless communication. These functions are realized through different ranges, bandwidths, and network coverage technologies, including 5G networks, FRMCS, satellite communication, Bluetooth, near-field communication (NFC), and others. However, all wireless transmission technologies are vulnerable to jamming attacks since they utilize radio waves that are accessible to everyone. Therefore, jamming will remain an attractive attack scenario in the future because current defense strategies and resilience concepts do not sufficiently hinder or prevent successful jamming attacks.

5.2. Countermeasures with a Further Need for Research or Standardization

Our work aims to investigate necessary countermeasures that keep the future railway system secure and identify those countermeasures where further standardization and research are required. Hence, after creating the 21 Attack Graphs, we identified countermeasures that reduced the risk to an acceptable amount. Countermeasures were given values of how much they reduced the risk by rating how much they either increased the necessary knowledge or resources to perform the attack successfully or how they decreased the impact caused by a successful attack. This resulted in a list of 49 desired countermeasures and direct visualization of resulting risk mitigation in the case of successful applications to the identified abuse cases.

These 49 countermeasures mitigated at least one threat described in Section 5.1. Some of these relations resulted from a single attack path in one of the 21 Attack Graphs. To discuss all relations in detail, we would therefore need to include the Attack Graphs, which we restrain from, as it would exceed the scope of this article. However, the Attack Graphs that describe the threats are already published and available online (<https://github.com/INCYDE-GmbH/attackgraphs> accessed on 22 September 2023).

Subsequently, we estimated the maturity of the 49 countermeasures, i.e., to which degree the countermeasure is already in use or ready for use in current railway systems. We use three maturity levels based on the well-known technology readiness level (TRL) [21]:

- A. The technology is in an early development or research state, meaning that there is, at most, a laboratory experiment (TRL 1–4).
- B. First prototypes of the technology exist (TRL 5–7).
- C. The technology is well-known and used; there is no need for further standardization or research (TRL 8–9).

To estimate the maturity level, we use three different standards to verify if they also demand the respective countermeasures. The standards used are as follows:

1. The IEC 62443 series [19];
2. The BSI IT-Grundschutz [22]; and
3. The concretization of requirements for critical infrastructures (CIs) [23].

After determining the maturity level, we discovered that 21 out of 49 countermeasures have level “A” or “B” and, thus, are not yet mature enough to secure real-world railway systems. Thus, for these 21 countermeasures, there is either some research demand to develop the technology further, they need to be better reflected in standards, or both. We further group the 21 countermeasures into six categories in Figure 3:

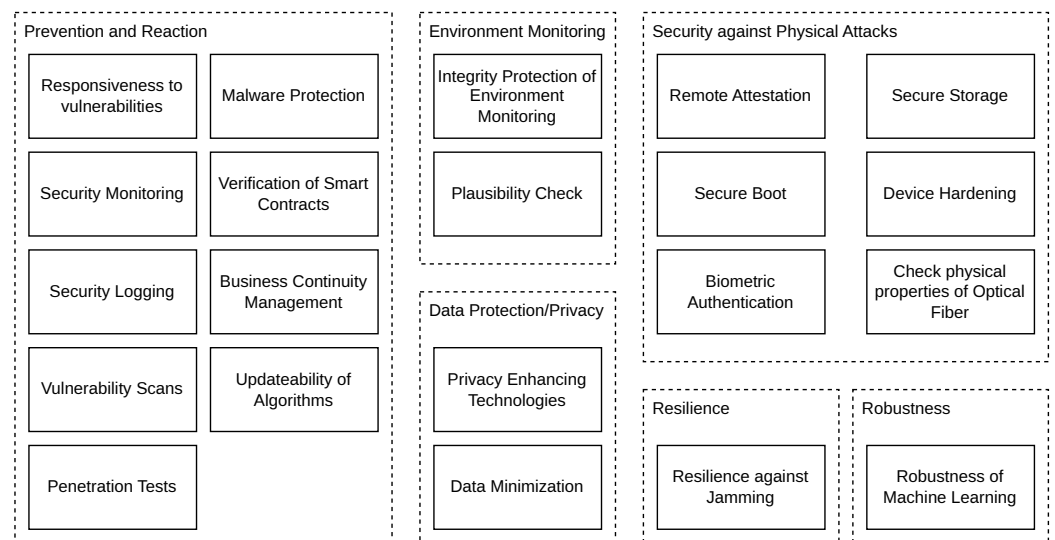


Figure 3. Countermeasures with a further need for research and standardization accumulated into six groups.

A total of 28 countermeasures that are already in use or deployed and are required by the standards have been identified. For some use cases, these existing countermeasures are sufficient, according to our risk evaluation, to reduce the risk to an acceptable level. In this case, the search for possible countermeasures was stopped, with an acknowledgment that there might be more or other well-established technologies to reduce the risk. However, as the goal was to identify the necessary demands not covered by state of the art solutions, we did not aim for the completeness of existing and standardized technologies.

Our work’s purpose is to identify the necessary research and standardization needs, rather than determining the potential for improvement. As such, we did not conduct a security evaluation for countermeasures that are currently in use or anticipated to be used. We operate under the assumption that countermeasures are correctly and adequately applied to mitigate risks. This holds true for both existing and future countermeasures. For example, we assume if encryption is necessary to reduce the risk of a threat; an encryption algorithm is chosen that fulfills the system requirements, including the security requirements, instead of an outdated or even a broken one.

In the subsequent sections, the groups are described, including the necessary actions to raise the maturity level of the respective countermeasures.

5.2.1. Prevention and Responsiveness

A large group of countermeasures is devoted to activities that prevent cyberattacks and the ability to react to newly disclosed vulnerabilities and a changing attack surface. Concepts for the ability to react to detected security issues already provide vital countermeasures that help to prevent further successful cyberattacks.

An essential class of cybersecurity threats is provided by malware infection. Therefore, malware detection and prevention (see, e.g., [24]) play important roles. While most standards already demand malware protection, an adequate implementation cannot yet be found in many systems of railway applications due to long system life cycles (legacy systems), lack of update possibilities, the requirement for readmission in the case of software changes, and the absence of software solutions for certain types of platforms. Research should investigate and define appropriate levels of protection against malware, which does not necessarily result in the development or adaption of anti-virus software.

If an attack is successful, systems should be fail-safe or fail-operational. This property is supported by business continuity management (BCM), which was already considered for IoT [25]. As demanded by BCM (compare ISO 22301 [26]), disaster recovery plans are not yet fully developed and tested for railway applications. Relevant systems need to catch up to state of the art BCM to maintain the availability of railway transportation, especially the parts that are considered CIs'.

Critical systems must be frequently examined for potential vulnerabilities that are helpful for an attacker. Vulnerability scans provide this. Furthermore, prevention can be reached by testing the execution of cyberattacks. In the past, these penetration tests were also considered in the area of IoT networks [27]. Both vulnerability scans and penetration tests are ready for deployment. However, field tests in railway applications are still pending to elevate the maturity level.

Further preventive countermeasures are provided by the continuous observation of the actual system's security state. In the first step, security logging is performed to collect and note all possible security-relevant system state information. Security monitoring is not yet applied in railway systems, even though there are proposals for doing so [28]. This provides functionalities like intrusion and anomaly detection as well as intrusion prevention. Security monitoring was already investigated along with networked control systems [29].

New developments may require the update of used algorithms, e.g., in the context of cryptography. Therefore, the ability to update algorithms is another countermeasure in the responsiveness category. As system life cycles can last over decades in railway transportation, it is necessary to provide a sufficient margin in the system's capabilities to incorporate future security controls, such as improved cryptographic algorithms.

To detect and prevent malicious modifications of smart contracts, the verification of smart contracts is another important preventive countermeasure. Formal methods to perform this task have already been investigated [30].

Most of these countermeasures can already be found in several standards. However, others are not standardized sufficiently, like the ability to update algorithms, or are not even mentioned at all, like the verification of smart contracts. Hence, to increase the maturity, some countermeasures still need to be standardized, while others need to be adapted for and applied throughout the railway systems.

5.2.2. Environment Monitoring

Proper and secure monitoring of the environment provides important security protection in railway systems. This includes the provision of integrity for any measured environmental data and conducting plausibility checks, i.e., checks for abnormal data values that are suspicious of manipulation.

Regarding the integrity of environmental data, some rules can already be found in all three investigated standards. However, some security issues were identified that were not adequately addressed by the existing standards, leaving them exposed to significant risks.

Furthermore, the technologies and methods used to ensure the integrity of environmental data are not applied consequently enough throughout the railway industry. In particular, in scenarios where safety-critical decisions are (semi-)automatically drawn from digitally captured environmental data, harmful consequences need to be avoided by a proper security concept. Examples include track clearance detection of automated trains, a train's digital twin used for predictive maintenance (implying safety responsibility), or detecting people (not necessarily identifying them) to avoid congestion in crowded areas.

No specific or relevant solution or regulation can be found to validate data using multiple input sources. This is because the technology for environmental recognition is still being developed and tested; it is not widely deployed. Hence, technologies and methods for plausibility checks must be further researched and standardized. This implies that these technologies must also be applied in the railway domain.

5.2.3. Security against Physical Attacks

Physical security covers all countermeasures, ensuring proper and secure functionality of technical processes or mechanisms protecting the system against physical access by unauthorized persons.

A proper system start may be provided, e.g., by Secure Boot, to ensure that attackers with physical access to a device cannot change the executed programs to mount an attack. While Secure Boot may be available for many systems, it must still be applied to many of our use cases, especially in operational technology (OT) and consumer devices. For protection against unauthorized access, remote attestation [31] can be used to verify to third parties that the software running on a particular device remains unaltered.

A further countermeasure is provided by biometric user authentication, in particular, voice recognition in connection with speech commands, together with ML. Our identified standards only briefly touch on the topic of biometrics but without closer consideration of our specific context or specific methods. Voice recognition systems for different application areas are already in use, but solutions to our specific context of ML still need to be developed.

By hardening devices or providing secure storage for cryptographic keys, further unauthorized physical access can be prevented. Trusted platform modules (TPMs) are standardized solutions for secure key storage. However, other standardized solutions must be provided since TPMs are not always feasible.

Fiber optic sensing (FOS) is an emerging technology in the railway sector [32]. While more decisions are based on the measurement results of FOS, the attack surface on the system increases. Physical manipulation of FOS could be countered by continuously monitoring the (physical) properties of the fiber up to the extent of a physically unclonable function (PUF) [33,34]. This group of countermeasures also includes particular technical disciplines away from current cybersecurity methods, which are out of scope for our considered standards. Before using these countermeasures, both the physical properties to be inspected and the inspection methods require more standardized guidelines.

Considering physical attacks and the introduction of countermeasures for physical security that already started during the engineering process, the security functions must run on the same hardware as the actual service [35] to provide sufficient physical protection. This can be challenging, especially in OT domains such as railway transportation, which is subject to the authorities' control, which can be challenging. While the remaining risks stemming from physical attacks are widely accepted today, this assessment will likely change due to the increased scalability of digital-physical attacks. Foundations to encounter such attacks are subject to research [28,35,36], but solutions have not yet transpired into operational systems. Hence, more research and development are needed to implement adequate protection against physical attacks on digital systems.

5.2.4. Data Protection and Privacy

As part of the transportation system, the railway industry handles the sensitive data of individuals and companies alike, including personal data, payment data, and location data of individuals. The data need to be protected to ensure the rights and privacy of all involved, while business models of stakeholders depend on gathering and sharing such data.

Privacy-enhancing technologies (PETs) aim to protect sensitive data while maintaining usability for interested parties [37–39]. A further strategy is data minimization, i.e., the avoidance of using unnecessary data. Privacy in connection with public transportation was already covered in the literature [40,41].

Neither PETs nor data minimization is covered in the standards relevant to the railway domain. Data minimization is only covered in the BSI IT-Grundschutz-Compendium [22] in regard to web browsers. However, the data mentioned above are not only handled via web browsers; possible scenarios include more data of those kinds from various sources and for mixed-use. Parts of the data might also have to be shared with other companies. Apart from the necessary standardization that needs to be conducted, methods and technologies need to be further improved to handle private data accordingly.

5.2.5. Resilience against Jamming

Wireless communication plays a significant role in the railroad area, and this communication is heavily susceptible to jamming attacks. Therefore, resilience against jamming is a vital countermeasure.

For CIs, detecting jamming attacks already provides a vital step [42]. Fallback strategies—either to other carriers or backup processes, to maintain the railway service’s availability—need to be developed and implemented to mitigate the consequences of a jamming attack. Beamforming seems to be a promising way to realize resilience against jamming [43–45].

However, resilience has not yet been covered in the relevant standards. The possibility of counter-jamming must be researched, developed, deployed, and standardized to increase maturity.

5.2.6. Robustness of Machine Learning

For a couple of use cases in the railroad sector, ML will play an important role. Hence, the robustness of ML is another essential countermeasure. Defenses against attacks on ML are often referred to as adversarial machine learning [20,46]. ML is closely connected with AI; a recent report detailing the current research requirements in this area was published by ENISA [47].

Adversarial ML and resilient AI are currently subjects of investigation. To ensure the correctness of future ML applications, further research is necessary in the railway industry, like using ML for predictive maintenance.

6. Conclusions and Future Work

Our research aimed to identify the research and standardization demands of security measures for future railway systems, as no such study exists today. Therefore, along with an expert team stemming from railway operators, railway manufacturers, and academia, we envisioned the potential landscape of railway systems up to 2050. We used 21 use cases by utilizing studies like the “Future of Rail 2050” by Arup Rail [12]. The use cases describe the utilized technologies and their connections, data flows, and benefits. These descriptions formed the basis of our subsequent security analysis, as no security analysis for these use cases has been conducted before. Therefore, we created an Attack Graph for every use case describing possible attack vectors and impacts. An analysis of these Attack Graphs showed that there are 14 frequently recurring attack scenarios. To ensure the security of future systems, we identified 49 security measures that are necessary to mitigate the threats and reduce the impacts of the attacks to an acceptable level. Another contribution of our

work involved identifying necessary research and standardization demands by rating the maturity of countermeasures. This resulted in 21 countermeasures, which we grouped into 6 categories based on the urgency of action required.

To adapt to upcoming security vulnerabilities, the prevention and detection capabilities of the systems need to be improved by security monitoring, BCM, and increased flexibility. Systems that rely on the perceptions of their environments must be hardened against falsification to maintain safe operation; this is accompanied by the need for increased protection against physical attacks, including measures like secure storage, Secure Boot, and remote attestation. The protection of PII is not yet in full force and it needs to be improved. Attention is needed on the resilience of all utilized wireless transmission technologies against jamming attacks, as well as the robustness of employed ML and AI against manipulation, including adversarial ML. Action must be taken by manufacturers, operators, and authorities of railway transportation authorities alike.

To conclude this article, we demonstrated the pressing need for research and standardization to secure the railway system of tomorrow. Future works should focus on investigating the identified security measures with the need for action, adapting them to railway systems. Furthermore, once the countermeasures are developed, they need to be standardized to ensure the security of all railway systems.

Author Contributions: Conceptualization, L.I., M.S. and S.K.; methodology, D.S., M.H., M.S., S.U. and S.K.; validation, D.S., L.H., M.H., M.S., S.U. and S.K.; investigation, D.S., L.H., M.H., M.S., S.U. and S.K.; resources, M.H. and S.U.; writing—original draft preparation, D.S., M.H. and S.U.; writing—review and editing, L.H., L.I., M.S. and S.K.; visualization, D.S., M.H. and S.U.; supervision, D.S., L.H., L.I., M.H., M.S., S.U. and S.K.; project administration, L.I., M.H. and S.K.; funding acquisition, M.S. and S.K.; All authors have read and agreed to the published version of the manuscript.

Funding: The presented work is part of the “Security Requirements Forecast and Evaluation of Possible Security Concepts” project, commissioned and financed by the German Centre for Rail Traffic Research at the Federal Railway Authority (2020-22-S-1202).

Data Availability Statement: Publicly available datasets were analyzed in this study. The data can be found here: <https://github.com/INCYDE-GmbH/attackgraphs>. accessed on 22 September 2023.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	artificial intelligence
ATO	automatic train operation
BCM	business continuity management
CBTC	communication-based train control
CI	critical infrastructure
COTS	commercial off-the-shelf
DAC	digital automatic coupling
DoS	denial-of-service
ETCS	European Train Control System
FOS	fiber optic sensing
FRMCS	Future Railway Mobile Communication System
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	global positioning system
IoT	Internet of Things
M2M	machine-to-machine
ML	machine learning

NFC	near-field communication
OT	operational technology
PETs	privacy-enhancing technologies
PII	personally identifiable information
PUF	physically unclonable function
RBC	Radio Block Centre
RIM	railway infrastructure manager
TPM	trusted platform module
TRL	technology readiness level
V2I	vehicle-to-infrastructure
V2V	vehicle-to-vehicle

References

1. Redaktions Netzwerk Deutschland. Ein Drittel Mehr Kapazität bei der Deutschen Bahn-so Soll es Klappen. Available online: <https://www.rnd.de/wirtschaft/ein-drittel-mehr-kapazitat-bei-der-deutschen-bahn-so-soll-es-klappen-X6M3WDPHKVIEFVMDHIIQAXOZU.html> (accessed on 11 July 2023).
2. Rebhan, C. Obwohl Regierung Mehr für Klimaschutz Tun Will: Erst 2022 Gibt der Bund Mehr Geld Für Schienen Aus Als Für Straßen. Available online: <https://www.businessinsider.de/politik/deutschland/obwohl-regierung-mehr-fuer-klimaschutz-tun-will-erst-2022-gibt-der-bund-mehr-geld-fuer-schienen-aus-als-fuer-strassen/> (accessed on 11 July 2023).
3. Iffländer, L.; Buder, T.; Loreth, T.; Villota, M.A.; Schmitz, W.; Neubecker, K.A.; Pickl, S. Physical Attacks on the Railway System. *arXiv* **2023**, arXiv:2306.00623.
4. Slivkova, S.; Michalcova, L. Identification and Classification of Soft Targets in Railway Infrastructure. In *Proceedings of the TRANSBALTICA XIII: Transportation Science and Technology*; Prentkovskis, O., Yatskiv (Jackiva), I., Skačkauskas, P., Maruschak, P., Karpenko, M., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 667–676.
5. Wang, Y.; Zhang, M.; Ma, J.; Zhou, X. Survey on Driverless Train Operation for Urban Rail Transit Systems. *Urban Rail Transit* **2016**, *2*, 106–113. <https://doi.org/10.1007/s40864-016-0047-8>.
6. Keevill, D. *Implications of Increasing Grade of Automation*; American Public Transportation Association: Washington, DC, USA, 2017.
7. Wunsch, S.; Lehnert, M.; Krimmling, J.; Easton, J. *Datenformate, Datenmodelle und Datenkonzepte für den Eisenbahnbetrieb*; Der Eisenbahningenieur; Eurailpress: Frankfurt am Main, Germany, 2016.
8. Schmit, M.; Kerth, S.; Sinnecker, G.; Walther, G. *Modernisierung des deutschen Eisenbahnnetzes durch Digitalisierung und ETCS-Ausrüstung*; Verband Deutscher Verkehrsunternehmen e.V. (VDV): Berlin, Germany, 2018.
9. Liu, Y.; Yuan, L. Research on Train Control System Based on Train to Train Communication. In *Proceedings of the 2018 International Conference on Intelligent Rail Transportation (ICIRT)*, Singapore, 12–14 December 2018; pp. 1–5. <https://doi.org/10.1109/ICIRT.2018.8641573>.
10. Toussaint, C. *Einsatz von Drohnen im Bahnbereich*; Der Eisenbahningenieur; Eurailpress: Frankfurt am Main, Germany, 2021.
11. Schmid, G.; Sendlhofer, G.; Lexhaller, M. *Robotik im Gleisbau*; Der Eisenbahningenieur; Eurailpress: Frankfurt am Main, Germany, 2019.
12. Chew, T.; Luebke, C.; Morrell, M.; Goulding, L. *Future of Rail 2050*; Arup: London, UK, 2019.
13. Leining, M.; Schubert, M.; Heinrich, M.; Katzenbeisser, S.; Unger, S.; Krauß, C.; Scheuermann, D. *Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte; Teil 1: Technologieprognose*; Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt: Dresden, Germany, 2022. <https://doi.org/10.48755/dzsf.220008.06>.
14. Eyben, F.; Wöllmer, M.; Poitschke, T.; Schuller, B.; Blaschke, C.; Färber, B.; Nguyen-Thien, N. Emotion on the Road: Necessity, Acceptance, and Feasibility of Affective Computing in the Car. *Adv. Hum.-Comp. Int.* **2010**, *2010*, 263593. <https://doi.org/10.1155/2010/263593>.
15. Costa, P.; Vasalou, A.; Pitt, J.; Dias, T.; Falcão e Cunha, J. *The Railway Blues: Affective Interaction for Personalised Transport Experiences*; ACM: New York, NY, USA, 2013. <https://doi.org/10.1145/2541831.2541843>.
16. Unger, S.; Arzoglou, E.; Heinrich, M.; Scheuermann, D.; Katzenbeisser, S. Risk Assessment Graphs: Utilizing Attack Graphs for Risk Assessment. *arXiv* **2023**, arXiv:2307.14114.
17. Heinrich, M.; Iffländer, L. Softwaregestützte Bedrohungsanalyse durch Angriffsgraphen. *Signal Draht* **2022**, *5*, 28–34.
18. DIN VDE V 0831-104:2015-10, Elektrische Bahn-Signalanlagen - Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443. Available online: <https://www.din.de/de/mitwirken/normenausschuesse/dke/veroeffentlichungen/wdc-beuth:din21:234969038> (accessed on 27 July 2023).
19. International Electrotechnical Commission. IEC 62443: Industrial Communication Networks—Network and System Security. Available online: https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf (accessed on 27 July 2023).
20. Huang, L.; Joseph, A.D.; Nelson, B.; Rubinstein, B.I.; Tygar, J.D. Adversarial Machine Learning. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, Chicago, IL, USA, 21 October 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 43–58. <https://doi.org/10.1145/2046684.2046692>.

21. National Aeronautics and Space Administration. Technology Readiness Level. 2019. Available online: https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level (accessed on 22 September 2023).
22. Schildt, H. *BSI IT-Grundschutz-Compendium Edition 2022*; Technical Report; Bundesamt für Sicherheit und Informationstechnik: Berlin, Germany, 2022.
23. BSI. *Konkretisierung der Anforderungen an die Gemäß § 8a Absatz 1 BSIG Umzusetzenden Maßnahmen*; Technical Report; Bundesamt für Sicherheit und Informationstechnik: Berlin, Germany, 2020.
24. Reznik, L. Malware and Vulnerabilities Detection and Protection. In *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security*; Wiley: Hoboken, NJ, USA, 2022; pp. 177–246. <https://doi.org/10.1002/9781119771579.ch4>.
25. Ali, J.A.; Nasir, Q.; Dweiri, F.T. Business Continuity Management Framework of Internet of Things (IoT). In Proceedings of the 2019 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 26 March–10 April 2019; pp. 1–7. <https://doi.org/10.1109/ICASET.2019.8714483>.
26. ISO 22301:2019. Security and Resilience—Business Continuity Management Systems—Requirements 2019. International Organization for Standardization: Geneva, Switzerland, 2019.
27. Johari, R.; Kaur, I.; Tripathi, R.; Gupta, K. Penetration Testing in IoT Network. In Proceedings of the 2020 5th International Conference on Computing, Communication and Security (ICCCS), Patna, India, 14–16 October 2020; pp. 1–7. <https://doi.org/10.1109/ICCCS49678.2020.9276853>.
28. Heinrich, M.; Götz, A.; Arul, T.; Katzenbeisser, S. Rule-based anomaly detection for railway signalling networks. *Int. J. Crit. Infrastruct. Prot.* **2023**, *42*, 100603. <https://doi.org/10.1016/j.ijcip.2023.100603>.
29. McParland, C.; Peisert, S.; Scaglione, A. Monitoring Security of Networked Control Systems: It's the Physics. *IEEE Secur. Priv.* **2014**, *12*, 32–39. <https://doi.org/10.1109/MSP.2014.122>.
30. Maffei, M. Formal Methods for the Security Analysis of Smart Contracts. In Proceedings of the 2021 Formal Methods in Computer Aided Design (FMCAD), New Haven, CT, USA, 19–22 October 2021; pp. 1–2. https://doi.org/10.34727/2021/isbn.978-3-85448-046-4_3.
31. Banks, A.S.; Kisiel, M.; Korsholm, P. Remote attestation: A literature review. *arXiv* **2021**, arXiv:2105.02466.
32. Du, C.; Dutta, S.; Kurup, P.; Yu, T.; Wang, X. A review of railway infrastructure monitoring using fiber optic sensors. *Sens. Actuators A Phys.* **2020**, *303*, 111728.
33. Maes, R.; Verbauwhede, I. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security: Foundations and Practice*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 3–37.
34. Gao, Y.; Al-Sarawi, S.F.; Abbott, D. Physical unclonable functions. *Nat. Electron.* **2020**, *3*, 81–91.
35. Heinrich, M.; Vateva-Gurova, T.; Arul, T.; Katzenbeisser, S.; Suri, N.; Birkholz, H.; Fuchs, A.; Krauß, C.; Zhdanova, M.; Kuzhiyelil, D.; et al. Security Requirements Engineering in Safety-Critical Railway Signalling Networks. *Secur. Commun. Netw.* **2019**, *2019*, 1–14. <https://doi.org/10.1155/2019/8348925>.
36. Heinrich, M.; Renkel, D.; Arul, T.; Katzenbeisser, S. Predicting Railway Signalling Commands using Neural Networks for Anomaly Detection. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Lisbon, Portugal, 16–18 September 2020; Springer: Berlin/Heidelberg, Germany, 2020. https://doi.org/10.1007/978-3-030-54549-9_11.
37. D'Acquisto, G.; Domingo-Ferrer, J.; Kikiras, P.; Torra, V.; de Montjoye, Y.A.; Bourka, A. Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *arXiv* **2015**, arXiv:1512.06000.
38. Kaaniche, N.; Laurent, M.; Belguith, S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102807.
39. Heurix, J.; Zimmermann, P.; Neubauer, T.; Fenz, S. A taxonomy for privacy enhancing technologies. *Comput. Secur.* **2015**, *53*, 1–17.
40. Heydt-Benjamin, T.S.; Chae, H.J.; Defend, B.; Fu, K. Privacy for public transportation. In Proceedings of the Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, 28–30 June 2006; Revised Selected Papers 6; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–19.
41. López-Aguilar, P.; Batista, E.; Martínez-Ballesté, A.; Solanas, A. Information Security and Privacy in Railway Transportation: A Systematic Review. *Sensors* **2022**, *22*, 7698.
42. Álvarez, A.; Trapero, R.; Guilhot, D.; García-Mila, I.; Hernandez, F.; Marín-Tordera, E.; Forne, J.; Masip-Bruin, X.; Suri, N.; Heinrich, M.; et al. CIPSEC-Enhancing Critical Infrastructure Protection with Innovative Security Framework. In *River Publishers Series in Security and Digital Forensics; Challenges in Cybersecurity and Privacy—the European Research Landscape*; River Publishers: Aalborg, Denmark, 2019; Chapter 7, pp. 129–148. <https://doi.org/10.13052/rp-9788770220873>.
43. Khan, S.A.; Malik, S.A. Adaptive beamforming algorithms for anti-jamming. *Int. J. Signal Process. Image Process. Pattern Recognit.* **2011**, *4*, 95–106.
44. Yu, K.B.; Murrow, D.J. Adaptive digital beamforming for angle estimation in jamming. *IEEE Trans. Aerosp. Electron. Syst.* **2001**, *37*, 508–523.
45. Kong, Z.; Yang, S.; Wang, D.; Hanzo, L. Robust beamforming and jamming for enhancing the physical layer security of full duplex radios. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3151–3159.

46. Morgulis, N.; Kreines, A.; Mendelowitz, S.; Weisglass, Y. Fooling a real car with adversarial traffic signs. *arXiv* **2019**, arXiv:1907.00374.
47. Ntalampiras, S.; Misuraca, G.; Rossel, P. *Artificial Intelligence and Cybersecurity Research*; Technical Report; ENISA: Attiki, Greece 2023. <https://doi.org/10.2824/808362>.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.