Railway Cyber-Security in the Era of Interconnected Systems: A Survey

Simone Soderi, *Senior Member, IEEE,* Daniele Masti, Yuriy Zacchia Lun, *Member, IEEE,*

***Abstract*—Technological advances in the telecommunications industry have brought significant advantages in the management and performance of communication networks. The railway industry is among the ones that have benefited the most. These interconnected systems, however, have a wide area exposed to cyberattacks.**

This survey examines the cybersecurity aspects of railway systems by considering the standards, guidelines, frameworks, and technologies used in the industry to assess and mitigate cybersecurity risks, particularly regarding the relationship between safety and security. To do so, we dedicate specific attention to signaling, which fundamental reliance on computer and communication technologies allows us to explore better the multifaceted nature of the security of modern hyperconnected railway systems.

With this in mind, we then move on to analyzing the approaches and tools that practitioners can use to facilitate the cyber security process. In detail, we present a view on cyber ranges as an enabling technology to model and emulate computer networks and attack-defense scenarios, study vulnerabilities' impact, and finally devise countermeasures. We also discuss several possible use cases strongly connected to the railway industry reality.

***Index Terms*—Railway systems, network security, railway signaling, cyber ranges, cybersecurity assessment.**

I. Introduction

Railways have been one of the main commodities to move passengers and freight since at least the late 19th century. Nevertheless, operators have faced mounting pressure to meet ever-increasing performance and safety demands from the public [1]. On top of such targets, the awareness of cybersecurity themes has also changed. For these reasons, securing railway systems from cyber attacks has lately become a central issue for practitioners and the public, especially after recent news stories such as [2].

The cause for this abrupt need for answers is simple: while, in the past, railway systems often depended on specifically purposed electromechanical devices that operated in an air-gapped environment, newer infrastructures are often based on commercial-off-the-shelf systems that operate in a fully networked setting. This means that such new installations offer both a much larger attack surface and that attacks can be carried out with shallower knowledge than before. The reliance on shared infrastructures for the operations of multiple subsystems (e.g., both VOIP and signaling might use the same network infrastructure to carry information) amplifies this problem, making the possibility of *lateral movements* extremely relevant. This possibility is problematic because railway companies may operate (through the same shared infrastructure) Information and Communication Technology (ICT) services, which have also been hit by various attacks [3]. This scenario is not unique to the railway sector: many public infrastructures have become victims of cyber attacks in recent years.

Many proposals have arisen to address this issue. For example, in 2008, the "European Programme for Critical Infrastructure Protection" [4] was established to improve the security of *critical infrastructures*, which are defined as all those systems considered essential to maintaining the vital functions of society. Recently [5], debates for updating this Directive have restarted to deal with the present threat landscape. The target has been to include a much broader landscape of systems, including the transportation industry and the railway sector, and to champion a novel approach more focused on the resilience of overall integrated infrastructures rather than on the security of individual assets.

Indeed, considering that a successful attack on railway systems can result in the loss of the safety guarantees of the network [6], the rail transportation sector cannot ignore cybersecurity anymore and must start considering cybersecurity, physical security, and safety as intertwined aspects that cannot be dealt with separately. For these reasons, developing a new generation of methods for verifying and hardening rail systems has become of great practical and theoretical importance.

In this survey, we investigate how the industry has responded to such a challenge by:

- collecting the standards governing the many safety-critical subsystems that make up a complete railway network;
- recalling some of the most significant cyberattacks

This manuscript version is a post-print of the article accepted for publication in the IEEE Transactions on Intelligent Transportation Systems. Digital Object Identifier **10.1109/TITS.2023.3254442**.

This work was supported in part by Consorzio Interuniversitario Nazionale per l'Informatica (CINI) through the Research Project under Grant CA 01/2021 a.i. 2. *(Corresponding author: S. Soderi.)*

S. Soderi and D. Masti are with the IMT School for Advanced Studies Lucca, 55100 Lucca, Italy (email: simone.soderi@imtlucca.it; daniele.masti@imtlucca.it).

Y. Zacchia Lun is with the Department of Information Engineering, Computer Science and Mathematics (DISIM), University of L'Aquila, 67100 L'Aquila, Italy (email: yuriy.zacchialun@univaq.it).

carried out in recent years on railways systems;
- investigating the cybersecurity projects involving railway signaling systems
- investigating an approach based on *cyber ranges* to emulate and verify the security of networking systems similar to those used in the railway industry.

The paper is organized as follows: in Section II, we recall the main components of a railway system; in Section III, we introduce the facet of security in the railway sector in general and, in Section III-C, we discuss the relationship between safety and security. Section IV concludes with a novel methodology for performing cybersecurity assessments. In Section V, we report how cyber ranges can be valuable in performing cybersecurity assessments and propose some railway-centered scenarios that might be of interest for discussion and future work. In Section VI, we finally draw some final remarks and discuss further developments.

II. Railways as an integrated system

In a broad sense, railways can be defined as a collection of different systems whose purpose is to transfer passengers and goods on wheeled vehicles running on rails located on tracks. Such subsystems can be broadly collected into three families:

- **Railway infrastructure** comprises all the tracks (sometimes referred to as the *permanent way*), all the civil works, and the systems and premises that ensure the regular traffic flow. In literature, this latter component is often further divided to distinguish between the so-called "facilities and premises," which encompass stations, depots, and other similar facilities and *wayside systems* that operate along the lines, which encompass signaling systems, electrification facilities (which hardening is deeply interlaced with the security of the electrical grid as a whole [7]) and level crossings.
- **Rolling stocks** comprise powered vehicles (locomotives, single rail cars, shunters, etc.), engineering vehicles, and trailer vehicles.
- **Railway operations** encompass the technical duties performed to ensure trains circulate and the commercial operations that railway companies perform to ensure revenue [1].

Most tasks carried out in a railway company involve all those three subsystems simultaneously. This suggests that "holistic" approaches that favor securing the system as a whole [8] should be preferred to approaches that focus on securing a single component of the system without caring for its overall capability to accomplish its many tasks.

A. The dualism between safety and security

Safety is deeply ingrained into modern industry, and railway makes no exception. Indeed, railways and other transportation systems are classified as safety-critical since their failure may result in loss of human life or disasters of another sort. The design of this kind of system has traditionally followed a "safety above all" paradigm, meaning that, to be considered fit to be used, each component (and the system as a whole) must achieve a minimum Safety Integrity Level (SIL) [9], [10]. This means that specific design rules and test procedures must be implemented following a specific set of standards and norms, guaranteeing that the system continues to fulfill its safety requirements even in case of random failure.

Nevertheless, despite the observation that an insecure system has much fewer chances to behave in a safe manner, many widely adopted safety standards do not consider cybersecurity explicitly or, at most, only generically mention that implementers should include cybersecurity mechanisms [11], [12], [13] in their design[1].

This lack of guidance in such an otherwise pervasive recommendations framework, coupled with the high cost and the relative inapplicability of otherwise commonly adopted security frameworks in railway scenarios, however, has often pushed companies to consider security as an after-thought of the overall design process of new railways systems, an after-thought often delayed due to business and cost reasons [14], [15]. Such a "lazy" approach is perhaps even more surprising considering that the relative simplicity of accessing the infrastructure [16], coupled with the vast effect that successful attacks on railway infrastructures may cause on the public at large, makes the railway infrastructure a juicy target for all kinds of attackers, from state-sponsored actors down to "script kiddies." This strategy may even end up causing more problems in the long term since security specialists may have to work on infrastructures composed of a complicated landscape of systems whose overall functioning is linked to insecure-by-design architectures, possibly too old to be coupled with modern security solutions.

Indeed, railway infrastructure has been the subject of numerous attacks in recent years. In Table I, we summarize a few significant confirmed cybersecurity incidents that have affected or had the potential to compromise transportation operation safety. Looking at the Table, it is easy to see that while the operations and safety systems were the primary targets in the earliest incidents, the attackers' focus has shifted mainly toward ITC-related systems in recent times. Nonetheless, many recent attacks still significantly disturbed the transportation services as a whole, possibly due to undisclosed (or possibly even the simple fear of) lateral movement by the attackers.

B. Security landscape in the railway industry

The importance of the target and the relative lack of existing approaches to railway security has pushed many authors to propose analysis for various kinds of attacks and their possible mitigations, also within the academic community. We refer to Appendix B for a brief list of methodologies that can be used to analyze cybernetics

[1]We will come back to this issue later in the paper.

Table I
TIMELINE OF CYBERSECURITY INCIDENTS IN THE RAILWAY SECTOR WITH THEIR DESCRIPTION.

Date	Description
August 2003	A computer virus disabled the CSX Transportation headquarters in Florida, affecting signaling in thousands of km of railway line. This incident has also been referred to as the "Sobig" incident [17], [18].
January 2008	A teenager derailed four tram vehicles causing injuries to twelve people after hacking a train network of Lodz, Poland [2].
December 2012	A cyberattack on a Northwestern US rail company's computers disrupted railway signals for two days [19].
March 2015	The HoneyTrain Project recorded over two millions logins attempts with four successful illegal accesses to the Human-Machine Interface (HMI) of a virtual train control system in the space of six weeks [20], [21].
Febraury 2016	BlackEnergy and KillDisk malware infected the systems of a prominent Ukrainian rail company. In December 2015 the Ukraine power grid cyberattack was also attaked using the same malwares [22].
July 2016	A study reported that the UK Network Rail had been hit by at least four significant cyberattacks over 12 months, including intrusion in rail infrastructure itself. According to such a study, these attacks seemed to be exploratory [23].
November 2016	A ransomware attack took ticket machines of the San Francisco light rail transit system (SF Muni) offline for a day, There was no impact on transit service, the safety systems, or customers' personal information [24], [25].
May 2017	Deutsche Bahn, suffered a ransomware attack on its data systems [26]. The same computer virus also hit the national railway systems in Russia [27] and China [28].
October 2017	Sweden's transportation Administration was targeted by a DDoS attack on the IT systems that monitor railway traffic. Two DDoS attacks hit the public transportation operator Västtrafik the next day [29].
May 2018	The Danish operator DSB came under a DDoS attack, making it impossible to purchase tickets. Internal mail and telephone systems used by the DSB staff were also affected [30].
March 2019	An Israeli cyber threat intelligence company identified an actor operating on a top-tier dark web forum selling access to an administrative panel of a Chinese rail control system [31].
October 2020	A ransomware attack hit the Société de transport de Montréal (STM) compromising 624 operationally sensitive servers. The outage also affected STM for over a week [32], [33].
December 2020	A ransomware attack hit OmniTRAX. It was the first publicly disclosed case of a so-called double-exhortation ransomware attack against a US freight rail operator [34].
December 2020	The Egregor ransomware attack hit TransLink, forcing the company to shut down several IT services including part of payment systems [35]. No transit safety systems were affected, but the IT problems impacted GPS functions on buses [36] and information regarding personal banking social insurance information may have been compromised [37]
July 2021	A cyberattack on Iran's railroad system caused chaos across the whole country [38].
October 2021	The Toronto Transit Commission (TTC) became a victim of a ransomware attack, losing access to systems used to communicate with vehicle operators, online booking, etc. [39]. Subsequently, the TTC announced that personal information of (former) employees, may have been stolen [40].
March 2022	Italian Railway Operator Trenitalia and National infrastructure holder were affected by a "cryptolocker infection", causing disruption of service [41].
April 2022	Linked to events in the Russian-Ukranian conflict, "*a clandestine network of railway workers, hackers and dissident security forces went into action to disable or disrupt the railway links connecting Russia to Ukraine through Belarus*" [42].

attacks and to [14], [43] for an extensive analysis of many works centered around railway-specific scenarios.

Nevertheless, as Wang *et al.* [14] and Kour *et al.* [43] also report, the analyses done to this day are too often concerned with particular aspects of a single system. In other words, they work without caring for the overall picture and context in which they are inserted, thus not considering how interactions between coupled systems may amplify or negate some threats. In this era where railway systems are made of tens of separate interconnected safety and security-critical systems, this approach may result in analysis and countermeasures of limited applicability and effect.

This problem cumulates with the already mentioned lack of cybersecurity awareness in the often legally-binding standards used in the railway sector. To give some examples, the CENELEC EN 50159 [44], which is used to design communication between safety-related equipment, addresses topics such as message authenticity and integrity. However, it does not cover general cybersecurity issues like preventing overloading transmission systems or ensuring the confidentiality of safety-related information. Another example is the IEC 61508 [10], which can be considered the general standard for achieving the safety of electronic devices and is extensively used in the railway industry, which does not cover security issues [13]. Indeed both standards only mention that intentional malicious human actions must be considered and generically refer to the ISA/IEC 62443 [45] standard. A similar landscape can also be found concerning the technical norms governing control platforms doors and wayside control systems. For the former, the primary reference is the GB 50157-2003 [46], which again does not tackle security issues [13].

Authors and governing bodies tried to address this situation, yet before analyzing their proposal, it is meaningful to analyze the unique requirements of railway systems compared to ICT systems. Nowadays, railway projects heavily rely on classical Industrial Control Systems (ICS) to control electromechanical systems and automate industrial processes and operations in various applications. Such systems often include programmable logic controllers, data communication systems, and supervisory control and data acquisition. Securing IC systems poses different challenges

than securing pure ICT systems. Consider, for instance, the Confidentiality, Integrity, and Availability triad, a well-known model that defines the security requirements to support organizations in specifying the core security objectives of their systems [47]. As shown in Figure 1, while ICT security focuses on confidentiality to prevent stealing private information, ICSs are more concerned with data integrity and avoiding unplanned system outages that can disrupt production availability and profitability.

Communication between subsystems also plays a central role and is usually achieved through a transportation network managed via a central Operation Control Center (OCC), where many operational tasks are merged. Currently, there is no consensus about how to design such control centers [13], and many different OCC configurations have been designed following possibly incompatible standards. Among them, the APTA RT-OP-S-005-03 [48] is among the most used ones, yet it considers only physical security and provides no guidelines for cybersecurity. Moreover, compared to classical ICSs, the transportation sector poses even more importance to the concept of resilience [49] since the availability of each subsystem has a paramount priority.

There is also the question about *how* connectivity should be offered to each one of such components: in theory, railway communications could build on many different technological options. Nevertheless, while the use of dedicated technology was practically mandatory in the past, in recent times, there has been a solid push for the use of non-dedicated backbones and off-the-shelf technologies to reduce setup and recurring costs and speed up deployment [16]. Indeed, although modern connectivity technologies like the 5G offers many security features, it is yet to be understood if (and how) they can be adapted to the railway's needs. In the next Section, we will analyze some of these aspects in more detail.

Figure 2 depicts the interconnected nature of modern railway systems. In there, we can see how the functioning of railway subsystems is assured by a vast number of devices positioned along the line, all reporting to operators and central systems located in central control rooms. The same picture also shows how the connectivity between all these devices is potentially offered by means of a network infrastructure whose fundamental principles are not necessarily much different from the ones used in classical enterprise ICT settings. Such a network backbone is also possibly shared with other railway or ICT subsystems. In such a case, logical separations between the data fluxes can be assured by the use of Virtual Private Network (VPN) technology.

C. A deeper look on signaling systems

One of the systems where the role of connectivity is the most pervasive is signaling. For this reason, we will take this primary function, and European Rail Traffic Management System (ERTMS) in particular, as the case study for the rest of the paper.

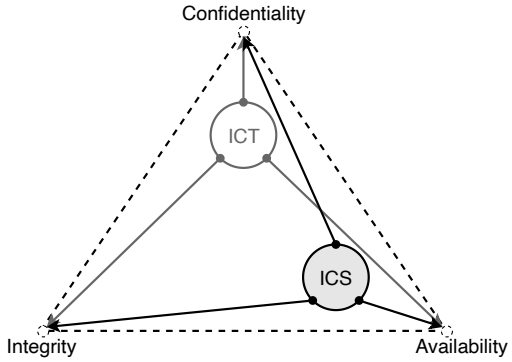

Figure 1. The different meanings of the Confidentiality, Integrity, and Availability triad in ICT and IC systems.

Signaling comprises all the machinery necessary to ensure the safe movements of rolling stocks on railway infrastructure [50] and is part of the so-called wayside systems. In detail, signaling systems are comprised of a few main components tasked to:

- check the clearance of track sections using either track circuits or axle counters;
- lock movable track elements such as switches and crossings in a proper position;
- prevent conflicting train movements through the action of an interlocking system. This system is responsible for granting a train exclusive access to a *route*, which is a sequence of track elements exclusively assigned for train movement through a station or a junction [51];
- controlling railway vehicles to keep them safely apart and within speed limits through Automatic Train Control (ATC) systems.

ATC systems can be further divided into three subsystems: Automatic Train Protection (ATP), Automatic Train Supervision (ATS), and Automatic Train Operation (ATO) [52]. ATP is a vital subsystem that continuously ensures compliance with the maximum safe speed and minimum safe distance limits. ATS often acts upon the signals generated by the interlocking system to monitor and adjust the performance of individual trains to ensure smooth railway service. The ATO subsystem performs those functions otherwise assigned to the train operator and meets all operating conditions and limits set by the ATC, following the requirements of the railway system to ensure passenger comfort by establishing policies for safe operations [51]. All modern railway signaling systems, such as the European Train Control System (ETCS) and Communications-based train control, include ATP functions [52].

Speaking about ETCS, such a system is used as the signaling and control component of the ERTMS, which is the *de facto* global standard [53] in the high speed and mainline railway market segment (please refer to Appendix A for an overview of the railway market).

The ERTMS standard has been designed to be an almost universal traffic management solution and specify

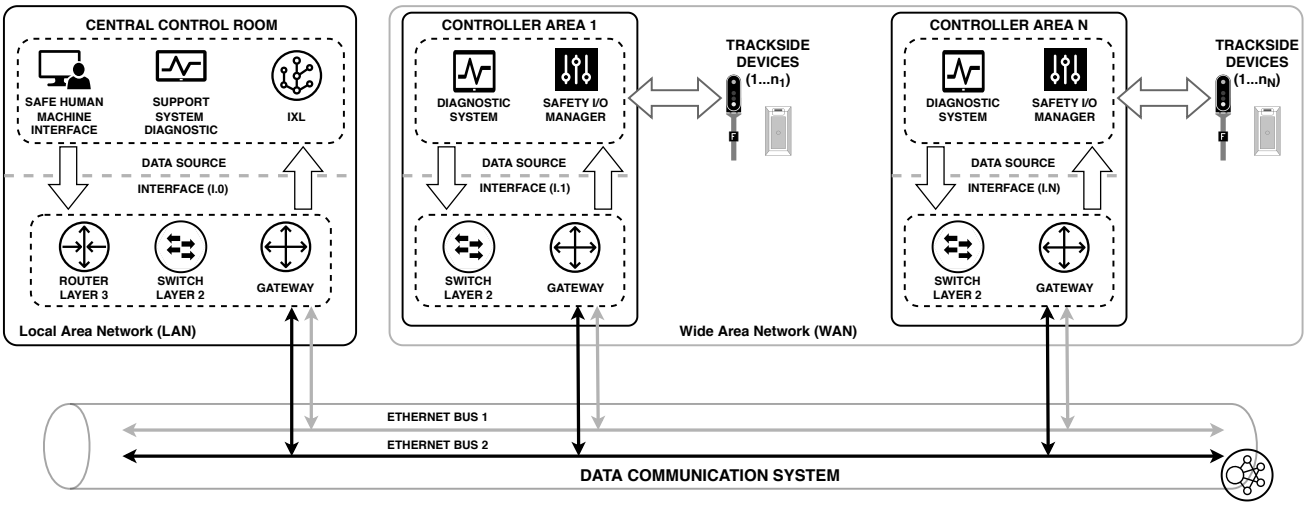

Figure 2. Wayside network scenario. The central control room connects the safe HMI with support system diagnostic and interlocking in LAN and controller areas via WAN. Each LAN comprises networking devices such as gateways, routers, and switches. The control areas link trackside devices to their safety input/output manager and diagnostic system.

several service levels, each of which enables more and more tasks to be accomplished by the system. The functions offered by different ERTMS range from none (in the case of a "Level 0") to a complete virtual train coupling system [54], which is the main subject of the possible future ERTMS/ETCS "Level 4".

This potential, however, has a cost in terms of the complexity and required capabilities of the employed communication channel. This, in turn, determines the type of equipment to be used [50]. At Level 1, for instance, the system relies on *intermittent* ATP architecture that uses controlled transponders ("balises"[2] or loops) positioned along the tracks. Such devices relay information received via a traditional signaling system via a Line-side Electronic Unit (LEU). At Levels 2 and 3, instead, the ETCS works as a *continuous* ATP system, which requires bidirectional Vehicle-to-Infrastructure (V2I) communication. In this case, railway cabs receive information from balises, short loop antennas, or digital radio[3].

To this date, the technology used as digital radio is the GSM-R system, which has been built on top of 2G GSM cellular technology. However, the GSM-R technology is starting to show its limits as it cannot provide enough support for growing ERTMS demands for autonomous train operation capabilities. For this reason, there has been a push to move to more advanced (possibly packed-switched) technologies. In this sense, a natural candidate would have been the LTE-R [56] (based on 4G cellular infrastructure), which has found successful applications in the Asian markets. However, as trains move faster and the quantity of data to transmit grows, it is easy to imagine scenarios in which even the current 4G technology would fall short. The novel "Future Railway Mobile Communication System" (FRMCS) [57], which relies on 5G technology, will probably be able to solve these issues. Nevertheless, in the meantime, the already mentioned LTE-R or the Finnish national "terrestrial trunked radio standard" (TETRA) [58], [59] are being adopted, even if only as stop-gap solutions.

[2]Eurobalise Transmission System is a safe spot transmission-based system conveying safety-related information between the wayside infrastructure and the train [55]

[3]Interestingly, thanks to the strong push on commonality, all ETCS levels use the same onboard equipment.

D. Security aspects of ERTMS

The central role of ERTMS (and signaling systems in a broad sense) in guaranteeing a safe circulation of trains has sparked the academic community to assess its security properties.

For instance, in [60], the Authors highlight weaknesses of GSM-R and EURORADIO protocols that would allow an attacker to forge train control messages. Although the Authors recognize that it would be challenging to carry out this kind of attack in an environment where only small segments of data are exchanged, their hypothetical attack will become a more pressing possibility in a context where the quantity of exchanged data will grow.

Another example is the attack proposed in [61], in which the authors exploit the fail-safe behavior of ERTMS to engineer a Denial-of-Service attack that causes a train to halt. Although the authors also argue that causing an accident might be possible, as shown in [14], also causing a delay for a single train can be enough to cause severe repercussions on the overall railway schedule and service.

More theoretical approaches have also been used to test the protocol's security (and safety). In [62], a formal analysis of the train-to-trackside communication protocols used in the EURORADIO protocol is carried out using pi-calculus and the ProVerif tool. In there, the Authors found out that the protocol is not secure against forging of emergency messages in all those cases in which the underlying carrier network is compromised (such as by an

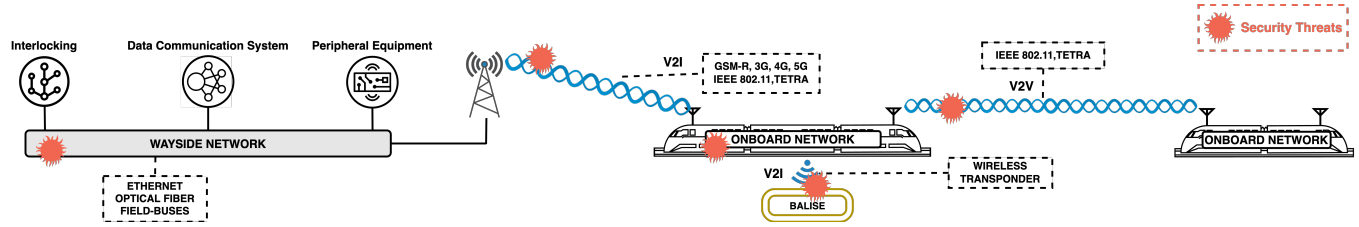

Figure 3. A schematic representation of the many communication channel used by railways systems. Dashed boxes list possible technological solutions. Each one of those links can be be potentially used to to carry out attacks to the connected subsystems.

IMSI catching in the case of GSM-R), and it is also weak against message deletion, and downgrading attacks.

Many authors have also proposed possible mitigation of known problems of these protocols. For instance, the very Authors of [62] make several recommendations further to enhance the security of ERTMS in the same paper. In [63], another approach to improve the protocol in EURORADIO is proposed by the Authors, accompanied by theoretical consideration employing Colored Petri Networks to verify the superior performance (both in safety and security terms) of their proposal.

Cryptographic considerations on the EURORADIO protocol and its coupling with various digital radio technologies have also been performed. In [16], for instance, it has been argued that the 3DES-based approach of EURORADIO is not secure enough given the nowadays available computational power. Attacks of this kind, however, often rely heavily on intrinsic properties of the GSM-R carrier and are thus heavily countered by the use of more modern carriers. We refer the interested reader to [16] for more in-depth considerations regarding the improved security primitives offered by LTE-R, 5G, and FRMC.

E. The limits of an atomistic approach

As already noted, all these analyses rarely take into account the overall placement of the analyzed system into the "operational pipeline" of a railway system. For this reason, they fall short of identifying the effects of a given attack on the railway system as a whole. Although acceptable in an academic setting, this approach is very myopic from a risk management point of view.

In Figure 3, we show a schematic representation of a railway system. Each component and each V2I, vehicle-to-vehicle, and spot communication channel can be subject to security threats. Wireless communication offers new possibilities for support and new services and also increases complexity during development as it exposes a broader attack surface. This picture is helpful to see how securing a single subsystem without regard for its placement in a general scheme may not achieve desirable overall security characteristics.

In an enterprise, there is also the urge to *quantitatively* investigate the effect of a given event. In systems as complex as railway signaling infrastructure, however, this feat is well beyond the possibility of a pencil-and-paper-based approach. Indeed, as noted in [14], simulators and verifiers have become invaluable tools for such a feat. Later in the paper, we will explore how *cyber-ranges* can be used to investigate how network conditions can propagate through a communication backbone and possibly disrupt the services which rely on it to accomplish their function.

III. Security assessment methodologies for railway systems

Although we cited only a few examples of possible attacks on a particular subsystem and cited just a few news events regarding successful attacks, it should be clear by now that railway players cannot simply ignore the security facets of the systems they operate.

As also mentioned, compared to a purely academic setting, the concept of *governance* (i.e., procedures, management, and certifications) assumes a more prominent role in an enterprise setting compared to the sheer discovery of novel vulnerabilities. This is even more true for companies operating in a setting where safety management has always played a primary role.

Given this premise, it should be no surprise that in recent times there has been a strong push also for developing cybersecurity *risk management* procedures.

In the remaining of this Section, we report some of the most relevant industry standards that one can apply in the rail industry and then introduce the general ideas behind these industrial schemes[4]. Later we will also introduce an original approach to achieve such a feat.

A. Standards for cybersecurity assessments

Currently, procedures for security assessment of railway systems are mostly framed within the ISA/IEC 62443 standard [45], which is the global standard for network security of industrial control systems. Such a document guides ICS operators through a pipeline that establishes all the requirements, controls, and best practices necessary for securing industrial networks.

Other generally applicable norms and frameworks regarding cybersecurity are:

- the Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408 [64]. This standard introduces security specifications, implementation, and evaluation procedures tailored for the designated use environment;

[4]Nevertheless, it must be noted that recently also Academia has started answering to this call as well. See, for instance, [14].

- the ISO/IEC 27001 [65] standard, which specifies requirements for establishing, implementing, and maintaining information security management systems;
- the Cybersecurity Framework (CSF) [66]. CSF consists of standards, guidelines, and best practices related to cybersecurity risk management. It also provides a common language for communicating cybersecurity expectations and awareness within and across organizations.
- the Open Source Security Testing Methodology Manual [67] (OSSTMM), which is the de facto standard for vulnerability assessment thanks to an auditing methodology aimed to satisfy regulatory and industry requirements.

All those standards and frameworks, however, are rather generic and not tailored to the needs of railway systems. To address this issue, the European Networks and Information Systems Agency has established a series of specific security requirements and measures for the operators of essential services that can be recast in the frameworks mentioned above [68].

B. Guidelines to enhance the security of railway systems

Players like the UK Department for Transport, the International Union of Railways, etc., have also produced some guidelines especially centered on the security facets of railway systems [69], [70], [71]. Bloomfield *et al.* [72] also provided a high-level cybersecurity risk assessment procedure for generic ERTMS-based railway infrastructures and ETCS onboard systems. Several projects have also tried to address the rail sector cybersecurity challenges under the Shift2Rail [73] initiative, a European public-private joint undertaking for rail research. In particular, the two arguably most significant projects under this umbrella have been:

- 4SECURail [74], a project that addresses the call for formal methods in the railway environment and supports implementing a computer security incident response team for railways;
- CYRail, which has produced various guidelines to enhance the security of railway systems [75];

but also X2Rail-1 [76], Roll2Rail [77], and Safe4RAIL [78], [79] projects are worth to be mentioned.

Moreover, we cannot not mention the NIST Special Publications Series 800, particularly the NIST SP 800-53 [80], which includes the NIST CSF security controls. We also cite the NIST SP 800-82 [81] deals with ICSs security controls often used for security in railways.

C. The issue of safety certification

Given the complicated and hyper-connected nature of modern railways systems, it is no surprise that companies have adopted a landscape of solutions relying on standards both from ITC and Operation Technology (OT) domains to secure their systems. Although this approach follows a trend already in use in other sectors, such as avionics and automotive, it also poses clear challenges in integrating all the prescribed guidelines in the same design.

In Table II, we summarize some of the principal design-oriented guidelines currently in use in the railway industry. There, as anticipated, we can see a landscape of safety and security standards, which in some cases also have to coexist at a very intimate level. This need arises, for example, in the devices involved in signaling subsystems. In there, for instance, the object controller of a trackside device (see Figure 2) will necessarily have to work both in a fail-safe but also very secure manner.

Moreover, the issue of safety certification still stands: since no standard guidelines to certify the safety of security modules exist, certifying and including security hardware/software in actual railway projects is far from trivial. To address this problem, some Authors [13] suggested that manufacturers should physically separate the security modules from the safety modules. The novel CENELEC TS 50701 "Railway Applications – Cybersecurity" [82] is possibly the first attempt from a standardization body to solve such an integration issue. This technical specification is based on ISA/IEC 62443 and provides a tailored solution for the railway industry, including rolling stock, signaling, and infrastructure. CENELEC will assess this document in three years and possibly transform it into a standard [83].

Given the complexity of the safety process defined by EN 50126 [9] and of the cybersecurity process described by TS 50701, however, it is imaginable that the synchronization between safety and security will be pretty complicated, especially considering that the two processes certainly have different duration and that cybersecurity management is also a practically never-ending process. In addition, the system under consideration defined by TS 50701 might have a perimeter of application concerning the safety process.

These facts call for a radical shift into the working pipeline usually adopted by the railway industry as they make it basically mandatory to consider the security requirements of the final product from the very beginning of the design process.

A possible architecture that may be used to meet these requirements is shown in Figure 4. In such a design, a security *shell* protects the safety function [84]. This leaves the designer free to apply any relevant standard (possibly from Table II) to design each internal component but imposes that all communications must go through a security controller, which will also function as the only interface to its safety counterpart. Such an architecture is implicitly resistant, for instance, to a DoS attack because, even in the worst case, only the functioning of the security controller can be compromised, thus leaving any internal fail-safe mechanism intact. In addition, this architecture allows one to combine safety and security in a very streamlined way since the designers only have to worry about maintaining the (reciprocal) compatibility between the $I1$ and $I2$ interfaces that connect the two controllers.

Table II
REMARKS ON THE APPLICABILITY OF STANDARDS, FRAMEWORKS AND GUIDELINES IN THE RAILWAY INDUSTRY.

Standards and guidelines	Application area	Security	Safety
ISO/IEC 15408 [64]	IT	✓	
ISO/IEC 27001 [65]	IT	✓	
ISO/IEC 62443 [45]	OT	✓	
CLC/TS 50701 [82]	OT	✓	✓
NIST CSF [66]	IT, OT	✓	
NIST 800-82 [81]	OT	✓	
OSSTMM [67]	IT	✓	
CYRail [75]	OT	✓	
4SECURail [74]	OT	✓	
IEC 61508 [10]	OT		✓
EN 50126 [9]	OT		✓
EN 50159 [44]	OT		✓

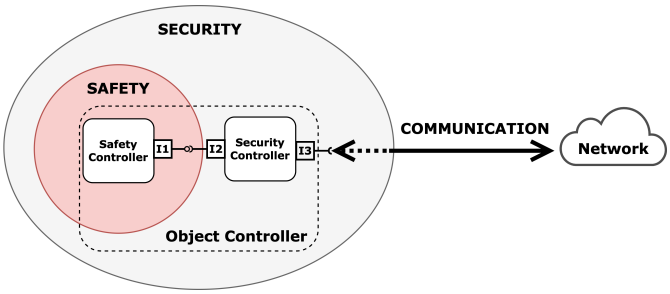

Figure 4. Example of a possible design architecture integrating both Safety and Security facets. In this approach, the security facets functions as external shell protecting safety function.

IV. AN ENTERPRISE-ORIENTED APPROACH TO SECURITY RISK MANAGEMENT

We have discussed how designers can make their design more secure, but what can a railway operator do to make its *systems as a whole* more secure? In other words, how can operators manage the overall cybersecurity risk?

It is obvious that this task involves both a governance and a technical part, in which the former is tasked to decide the high-level targets involving the security posture of the company and to decide the internal organization and scope of the cybersecurity teams. The kind of organization usually adopted often follows a hierarchical structure and is tasked to convert the high level decision imposed by higher management into a series of requirements regarding both the materiel and the operating procedure of the company. In turn, these requirements will be usually met by applying the relevant standards, such as the ones we discussed in the previous Sections.

From a technical point of view, the first steps of this process involve performing a *security analysis* of the existing systems to identify weaknesses in the system [82]. This step will encompass identifying risk scenarios, computing the unmitigated risk, and finally mitigating it. To do so, the cybersecurity assessors rely on standards and their experience to gauge the strength and effectiveness of the company's security posture.

There are different types of these assessments [85]. For instance, when an organization's internal teams perform such an evaluation, we speak about *cybersecurity assessment*. Its main goal is to understand the sources of threats, threat events, and possible vulnerabilities on different levels. This process will encompass almost all aspects of a company, spanning from security policies to network architecture and each device's intrinsic characteristics. When external experts conduct the analysis, instead, the focus is to measure the compliance of an organization's systems and processes against specific cybersecurity standards and criteria. In such a case, we call this analysis a *security audit*.

In both cases, Cybersecurity Risk Assessments (CRA) will be produced. CRAs categorize cyber risks by likelihood and impact and will be included in a final report directed to the company's management. Such a report will also be used as a base to write recommendations to improve the security posture of the company [85].

It is important to note that, regardless of the actor who performs the investigations, these kinds of processes tend to be highly disruptive to the normal workflow of a company. Consider, for instance, the process of assessing the vulnerability of a given subsystem. This feat will involve automated scans that create considerable traffic load and abnormal interactions in the target systems and probably trigger any system security management tool already present. This reasoning is even more actual for penetration tests: this technical methodology extends vulnerability assessments with sanctioned attempts to exploit the discovered vulnerabilities to show their potential real-world impact. In other words, a successful penetration test on live equipment can cause all the negative effects of a real successful attack.

It is then easy to see that security assessments of any kind must be seen as a project themselves: clear goals and scope must be established, and operative constraints must be taken into account. A clear communication and cooperation strategy between all parties must also be established to ensure that the overall processes cause no more disservices than absolutely necessary.

A. An applicative procedure for cybersecurity assessments

In this Section, we detail how a security analysis can be carried out. To do so, we take as a test case the network security analysis of a wayside systems[5] like the one shown in Figure 2. This procedure can be seen as a summarization of the rules in the standards/guidelines mentioned in Section III-A.

The first step of the procedure is the so-called *information gathering* phase. At this stage, one collects information regarding the system under concern, such as

[5]The scheme we present can also extend to onboard networks.

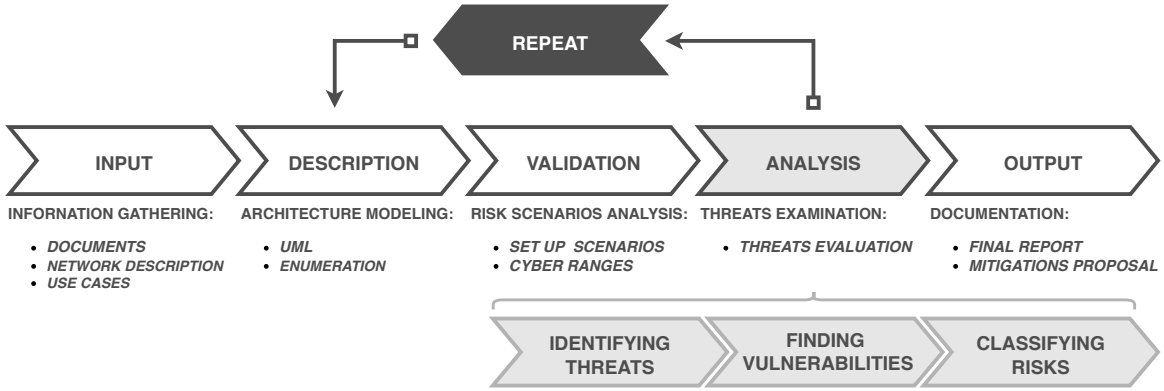

Figure 5. Graphical depiction of the general cybersecurity assessment process detailed in Section IV-A. The core stage is highlighted in gray.

requirements, technological assumptions, network characteristics, etc. These data will be used to extract a list of all network components and all interfaces that allow communication between them. Such analysis is the main object of the *architecture modeling* phase.

With such a scheme, one can further proceed with the *risk scenarios analysis*. Depending on the specific case, this step may involve auditing network device configurations, inspecting the policies already in place and real traffic, identifying protocol weaknesses, etc. The analysis of security requirements also takes place at this stage.

The subsequent step is the *threat examination* phase. At this stage, the auditor tries to identify the *threats* that might affect the network under test, namely all those circumstances that might disclose, manipulate, or destroy information, together with all those events that might result in a loss of network availability. This stage, in turn, comprises performing three steps, namely:

- *identifying threats* in software, protocols, and architecture is preliminary for determining the associated risks in the last step;
- *finding vulnerabilities* in software, protocols, and architecture. Specialized literature, such as the papers mentioned in the previous Section, and public repositories of Common Vulnerabilities and Exposures (CVE) [86] list, such as the one overseen by MITRE Corporation, are the most important sources at this stage.
- *Identifying the associated risk* that derives from the threat event's likelihood and the impact it might have on the network;

The cybersecurity assessment ends with a *report*.

An overall scheme of this procedure is shown in Figure 5. In the upper part, the main phases of the assessment are shown with a brief explanation of the involved step. In the bottom part, we instead detail the three subphases that comprise the Analysis step.

It is worth mentioning that the threat examination stage resembles the hazard analysis involving hazard identification and related risk analysis and evaluation in the safety assessment process (see [87] and the references therein). However, as described in Section II-A, the safety and security analyses differ in their focus.

It is also important to remark that, despite being based on the current literature, the procedure we presented in this Section is *novel* in the sense that it does not draw any specific elements from any other existing standard or scientific literature except for its general reasoning and principles. In other words, this is but one among the many possible choices to accomplish a cybersecurity assessment.

V. Cyber ranges as assessment tools

We mentioned how studying security threats is highly disruptive to do on live systems and possibly very challenging to carry out in a laboratory due to the sheer nature of the required equipment. This is especially true for network-centered subsystems.

With the term *Cyber ranges* [88], we indicate all those interactive platforms that allow one to create possibly entirely virtual representations (called *scenarios*) of existing ICT infrastructures and to emulate their operations by exploiting virtualization and digital twin technologies. Compared to a classical pure experimental laboratory setup, the heavy use of such technology cuts setup and running costs and allows one to operate scenarios also in a totally remote manner.

Scenarios represent a particular combination of active elements, configurations, selected interconnections, and any other specific information required to fully emulate a system. It is obvious that to faithfully reproduce complex systems, just like in the case of physical reproductions, a critical challenge is obtaining highly detailed knowledge from the system owners about their systems. This means that, almost ironically, the first benefit one gets when building such virtual scenarios is thus not technological since it forces both owner/operator and security assessors to detail the internal functioning of the original system [89].

A. The landscape of cyber ranges

Many solutions have been proposed to create cyber ranges, depending on the complexity, typology, and purpose of use. To better assess the technological landscape,

Figure 6. Graphical depiction of the working pipeline adopted to perform vulnerability assessments using a cyber range.

an idea is to distinguish between cyber ranges based on *simulation-based* architectures from those based on *emulation-based* architectures. The difference is that a simulation environment mimes the essential characteristics of the physical system but neglects low-level implementation details. Such details, however, may be crucial for a thorough network security analysis. Instead, an emulation environment reproduces most physical system peculiarities on a virtual platform.

When all the scenario components in a theater adopt virtualization solutions to emulate physical devices, some authors classify them as *virtual*. *Physical* theaters provide a replica of the target infrastructure in an isolated and secure environment. *Hybrid* cyber ranges adopt solutions relying on a combination of hardware, virtualized, and simulated elements.

The development and execution of experiments in cyber ranges involve labor-intensive and error-prone operations. For this reason, most cyber ranges platform heavily rely upon automation [90], [91]. However, many commonly used off-the-shelf theater automation (also called *orchestration*) frameworks, and, in turn, the cyber ranges that exploit them, do not provide a complete set of network-related functionalities. Luckily, various examples of network-centered cyber ranges also exist. They, however, widely differ in performance and implementation methods. In Table III, we present a brief schematic comparison between some well-known network emulators[6].

Among the essential features that one would like to have in a cyber range, the capability of interacting with components that live outside the emulated scenario is of paramount importance. Although this might sound counter-intuitive since the isolation guarantees are one of the biggest selling points of cyber ranges, this feature is also crucial to test the interactions with non-emulable components (such as industrial supervisory control systems). This allows specialists to assess the effect of various otherwise non-easily testable vulnerabilities. We refer the interested reader to [92], [93] for further reading on the topic and to the PAIDEUSIS [94] project for an example of successful integration between a virtual environment and physical machinery.

B. The role of cyber ranges for network security

A use-case in which cyber ranges shine is enabling security testing of complex systems. For interconnected systems, for instance, they allow one to study how malware propagates on its network or to emulate the effect of an attack at L2 on a given link.

[6]A complete systematic review of cyber ranges landscape would be outside this work's scope.

Cyber ranges naturally fit in the workflow presented in Figure 5. Following the proposed procedure, the "description phase" entails enumerating the system components and modeling them in a cyber range-friendly way, i.e., in a way that configuration management and orchestration tools can immediately process (e.g., an specifically crafted YAML configuration file in the case of a cyber range orchestrated using Ansible [95]). If done right, this allows one to create scenarios and straightforwardly analyze the system vulnerabilities.

Security threats can have many faces: flawed network architecture, erroneous device configurations, weak protocols, etc. A significant advantage of cyber ranges is that, thanks to their high fidelity simulation capabilities enabled by virtualization technology, they allow practitioners to study how threats combine their effects in a way that would be practically infeasible for other approaches.

Conforming to the cyber kill chain approach (please refer to Appendix C for details), the workflow for using a cyber range to evaluate network security broadly considers the following steps:

1) emulate the network (or a part of it) using the actual configurations and operating systems of the involved devices;
2) research the vulnerabilities through automatic tools and scripts created for the specific case;
3) enumerate the vulnerabilities and measure their impact on the system under test.

Once one has found a vulnerability using the cyber range, the security analyst can proceed in developing a countermeasure and give evidence of it using the very same tools used for assessing the presence of vulnerabilities in the first place. This process will result in new scenarios that no longer contain the vulnerability and can be used for further analysis. The procedure can be repeated until the analysis has covered all the network segments.

Figure 6 depicts the methodology presented in this Section in a flow chart. In there, we stressed the often overlooked importance that orchestration tools assume in making ranges an actual practical instrument.

C. Building cyber ranges: an applicative example for railways and signaling

As a practical example of the proposed procedure, in this Section, we show how EVE-NG can be used to investigate an imaginary IP/MPLS[7] backbone like the one shown in Figure 7.

This kind of network is a realistic representation of what a railway operator may use to interconnect equipment in different stations and is inspired by [102], [103]. In the picture, we can distinguish a central core network representing the core routers of the backbone, possibly connected by high-speed fiber optic links that may span a country. The core is tasked to offer connectivity to, among

[7]A proper treatment of MPLS networks is outside the scope of this document. We refer the interested reader to [101] for further readings on the topic.

Table III
A schematic comparison between some well known cyber-ranges solutions: Cisco Modeling Labs (CML) [96], Common Open Research Emulator (CORE) [97], Emulated Virtual Environment - Next Generation (EVE-NG) [98], Graphical Network Simulator 3 (GNS3) [99], and Mininet [100]. All these emulators provide means for connecting external nodes, but only CML, EVE-NG, and GNS3 support device operating system virtualization.

	CORE	**Mininet**	**EVE-NG**	**GNS3**	**CML**
Network configuration	Python, Labs	Python, CLI	API, Labs	API, Labs	API, Labs
Network emulation level	L3, (L1/L2 EMANE)	L2	L2	L2	L2
Connection to external nodes	Yes	Yes	Yes	Yes	Yes
Nodes operating system emulation	No	No	Yes	Yes	Yes
Licensing	BSD	BSD	GPL, Commercial	GPL	Commercial

others, signaling boxes along the rail lines. Connections related to different services (signaling, alarms, etc.) are segregated using MPLS VPN technology, which ensures separation between the traffic generated by the different local area networks inside the signaling boxes. In each local network, we can recognize a customer edge router connected to the core and a firewall. This latter device guards the traffic flowing into each local area. This scheme describes, for instance, a situation in which many signaling boxes (the clients) are connected to a central OCC (not shown but conceptually identical) using VPN technology using a railway holder own infrastructure.

In the scenario, configurations for each device are managed via Ansible, meaning that configurations can be easily modified and applied to stress different aspects of the network, facilitating the discovery and assessment of vulnerabilities.

We remark that in this shown scenario, the devices are virtualized. Although this may cause more difficulties for the first setup, it also means that each component will actually behave like the real one instead of being a mere reproduction whose functioning may differ due to slightly different implementation details.

Reproducing this scenario in a cyber-range allows one to test the following cases:

Scenario 1 What would happen if an attacker could make one of the links in the core unavailable? Would the internal routing protocol of the core converge again fast enough to guarantee the continuous operation of the overlying systems?

Scenario 2 Would the same conclusion also hold in the case of a *flapping link*? Would the core be able to react fast enough, or would its transient behavior hinder the overlying applications?

Scenario 3 How does a given OT protocol works in case of a congested network? Does the degradation of the links cause violations of timing constraints, loss of information, etc.?

Scenario 4 How many resources can be consumed by DoS attacks on IT applications running on a separate VPN but sharing the same infrastructure? Would the necessary separation be maintained, or should QoS policies be implemented to ensure the functioning of OT applications?

Scenario 5 Would manipulating a given link by some means allow one to establish a side-channel information transfer? Would this possibly compromise the separation between VPNs?

Scenario 6 What would happen if an infrastructure key device is replaced by one from a corrupted node, as in [104]? Are other nodes governed by a given protocol capable of circumventing the problem?

Scenario 7 Does the overall employed control structure suffer from Zeno behavior [105] following some kind of momentous Denial-of-Service?

Scenario 8 Is the network configuration subject to a given CVE, or is the architecture able to prevent the effect of the exploit?

Scenario 9 What kind of application-level performance degradation would a given kind of electromagnetic interference on a device/link cause?

Obviously, not every cyber range is the right tool to test *all* those attacks. To test Scenario 9, for instance, one would require either a strict integration with FEM tools or the ability for the cyber range to work in a hardware-in-the-loop configuration. Similar considerations also arise from scenarios linked to emulating the physical layers, which would be required to practically evaluate solutions like the one in [106]: very few tools can do so. This should not sound discouraging: most cyber range suites are remarkably flexible and allow a great degree of customization of the scenario details. To give an example, a tool like EVE-NG can easily handle all the first eight scenarios with little difficulty.

A related thought must be brought up concerning *performance* considerations. It would be foolish, for instance, to expect a simulated environment to match the actual throughput of a couple of enterprise-grade routers connected via an actual fiber optic link. Nevertheless, this does not mean that performance-related investigation cannot be performed using this kind of tool. Indeed, even leaving aside the practical possibility of empirical "conversion rules" between simulated and real-world scenarios, there is no reason to believe that *relative changes* would not be realistically represented. This observation implies,

for instance, the cyber ranges' ability to quantitatively estimate the effect of *amplification attacks*: if one discovers in a scenario that an attack has a given amplification factor, it should be pretty straightforward to scale the quantities involved to discover the actual resources (such as bandwidth) that an attacker would need to use to cause problems in the physical world. Similar considerations can be drawn for all those scenarios (such as Scenario 1 and Scenario 2) where protocol delays or other algorithmic considerations dominate the behavior of the system. In such a case, the hardware mismatch would cause minimal issues.

The same reasoning also holds when it is needed to establish the *feasibility* of some countermeasures. Suppose, for instance, that we would like to test if solutions like public key infrastructures (such as X.509, although arguably ill-suited for OT applications [107]) or the proposal like the one [108] are too computationally heavy to be implemented within real-time constraints. Even if the actual run time of the cryptographic primitives may be distorted by modern CPU hardware acceleration, the number of packets exchanged due to the intrinsic functioning of protocols (such as handshakes) will be faithfully represented in the virtualized scenario. This allows, for instance, to establish if such handshakes are too time-consuming by simply considering the transport delay of a real country-spanning link and the number of packets exchanged.

Although all the aforementioned considerations could also be drawn using physical equipment, on a practical level, cyber ranges are the most cost-effective tool to enable companies to deploy internal cybersecurity teams (with both "blue" and "red" teams roles), thus allowing a proactive approach toward security. This capability enables organizations to train cybersecurity response teams to respond to attacks [109] carried out by different kinds of attackers (is the attack source internal or external to the network? Is it a one-person job or coordinated state-sponsored action?) in a relatively effortless manner [110], [111]. Indeed, the cyber ranges have already shown their potential as invaluable tools for training purposes [112], [94]: events such as the CyberChallenge.IT [113], which have become possible thanks to such tools, are witnesses to this fact.

VI. Future challenges and conclusions

In this survey, we have reviewed the current landscape regarding the cybersecurity of railway systems, with a special focus on signaling systems and noting how they strongly rely on complex communication networks.

To do so, we first analyzed the origin of the ever-increasing interest in new tools and methodologies for cybersecurity rapid risk assessment for safety-critical infrastructure and reviewed the guidelines that can be applied to rail signaling scenarios. We then proposed a novel cybersecurity assessment procedure and showed how one can heavily exploit cyber ranges as an enabling technology to create virtual scenarios in which each vulnerability can be tested and its impact/risk assessed. As a result, our assessment procedure can help improve the cybersecurity posture of railway systems by understanding and mitigating cyber threats and vulnerabilities.

Many questions remain open. The most pressing one is how to better integrate cyber ranges with digital twins. This would allow for an unprecedented level of fidelity and allow for simultaneously studying the safety and security aspects of the systems under concern. To this end, we will also need to address the computational requirements of high-fidelity simulation environments. Indeed, as the final goal would be to emulate a railway system in its entirety, it is easy to see how the required computational resources might be beyond the current state-of-the-art capability.

Another challenge is definitely on the cultural level: how can we train tomorrow's technicians? Gamification has been used in cybersecurity for many years as an analysis tool, but can it be used for proper training purposes? Cyber ranges can be powerful tools also to this end, so it will be interesting to see if and how railway companies will adapt to such tools.

Appendix A
An overview of railway market

In order to better understand the scenarios that a company may have to face when assessing the security profile of a railway system, it is helpful to introduce the way railway systems are often classified based on the intended task they are meant to achieve. The first distinction to be made is between passenger and freight rail services. Among the former, we can further distinguish based on the distance traveled and the kind of territory served (e.g., urban, inter-regional, etc.) Railway networks are often organized around mainline rails that serve as a route between major urban centers and to which branches, yards, sidings, and spurs are connected. Mainline is used to provide both High-Speed Rail[8] (HSR) services and conventional speed rail services. *Regional traffic* may or may not share the infrastructure with mainline traffic [116] and provides conventional medium/short-based services. Finally, an urban/sub-urban segment may share the tracks with ordinary road traffic and is often separated from the mainline rail traffic. Examples of such traffic are metros, tramways, and light rails.

Appendix B
Incidents and their modeling

Many authors have formally proposed approaches to analyze such cyber attacks to understand better the attack patterns used. We cite here attack graphs [117], trees [118], [119], vectors [120], surfaces [121], over and above diamond model [122], OWASP threat model [123], and the so-called "kill chain" approach. See, e.g., [124], [43] for an overview of some of these models and [125], [126] for applications of attack-fault trees to analyze some cybersecurity-related incidents in the rail industry. We also cite [127], [128], [129]

[8] An HSR service is defined as a service that achieves a speed [114] of at least 200 km/h, regardless of the distance covered [115].

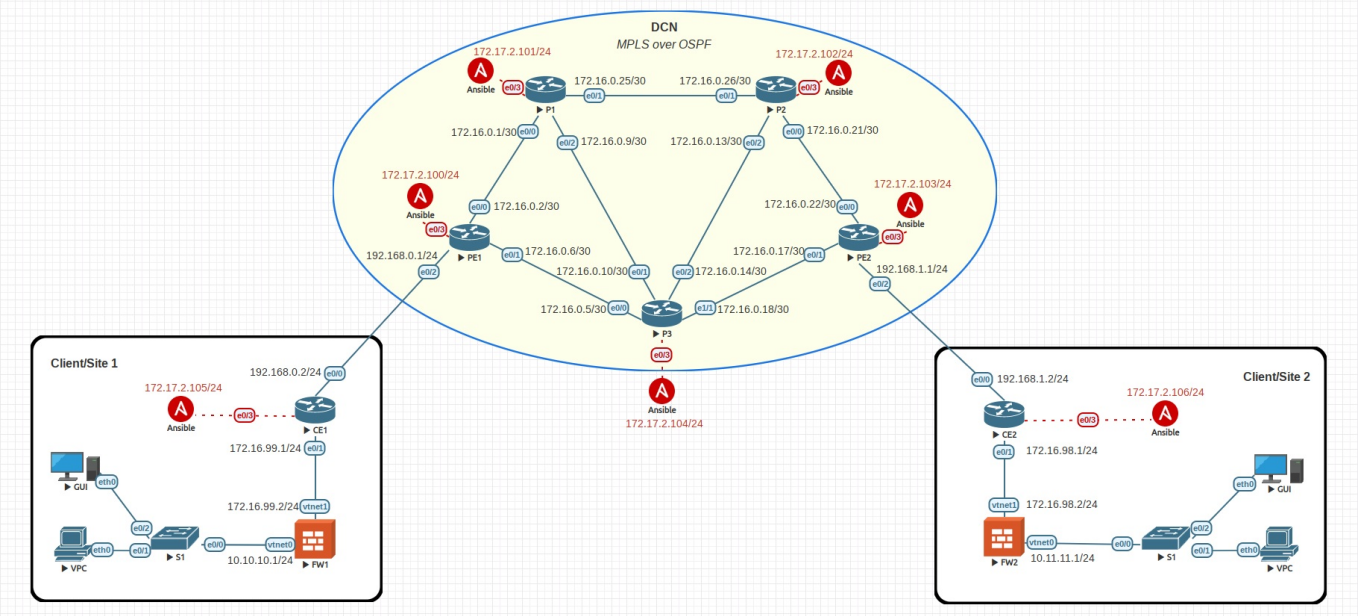

Figure 7. Example of using cyber-range to emulate an IP/MPLS network. The picture represents the network described in Section V-C.

for a reviewer on the security of cyber-physical systems from a control-theoretical prospective.

Appendix C
The cyber kill chain approach

The Kill Chain is a classic military concept that can be used to analyze the structure of an attack. More recently, Locked Martin introduced the same concept in the cyber domain context [130] to better model attacks involving network intrusions. It involves seven phases, each of which has a preferred mitigation approach.

According to the kill chain approach to modeling threats [131], cyber *reconnaissance* is the first step an attacker performs when trying to breach a system. There are two types of reconnaissance: passive and active. Passive reconnaissance is when the attacker gathers information about a target without direct interaction. Active reconnaissance is when an attacker directly interfaces with a target system to gather specific details that are later helpful in delivering a malicious payload. The subsequent phases are [132]: *weaponization*, in which the intruder creates remote access malware "weapons" tailored to one or more vulnerabilities; *delivery* of the weapon to the target; *exploitation*, which happens when the "weapon" is triggered; *installation*, which refers to the phase in which the weapon installs backdoors of various kind; *command and control*, in which the malware enables an intruder to have access to the target network. The last phase is referred to as *actions on objective*. Here the attackers take action to achieve their goals.

We refer the reader to [126], [131], [133] for a more detailed presentation of this topic and how kill chains can be used to analyze cybersecurity-related incidents, also in the rail industry.

Acknowledgments

The authors would like to thank Maurice H. ter Beek and Rocco De Nicola for their insightful comments.

References

[1] C. N. Pyrgidis, *Railway transportation systems: design, construction and operation*. Boca Raton, FL, USA: CRC press, 2016.
[2] J. Leyden, "Polish teen derails tram after hacking train network," *The Register*, Jan. 11 2008. https://www.theregister.com/2008/01/11/tram_hack/.
[3] H. Jo, G. Kim, J. Baek, K. Lee, D. Shin, Y. Shin, and J. Lee, "A study on the on-board centered train control system through ICT convergence," in *Proc. 12th Int. Conf. Control, Automat. Syst. (ICCAS)*, pp. 1206–1210, Oct. 2012.
[4] Council of the EU, "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," *Off. J. Eur. Union (OJ)–Legislation L)*, vol. 51, no. 345, pp. 75–82, 2008.
[5] "Proposal for a directive of the european parliament and of the council on the resilience of critical entities," *(COM (2020) 829 final)*, 2020. European Commission, Brussel, Belgium.
[6] D. Milligan, "Securing a railway control system," in *Proc. 9th IET Int. Conf. Syst. Saf. Cyber Secur.*, pp. 1–6, IET, Oct. 2014.
[7] S. M. M. Gazafrudi, A. T. Langerudy, E. F. Fuchs, and K. Al-Haddad, "Power quality issues in railway electrification: A comprehensive perspective," *IEEE Trans. Ind. Electron.*, vol. 62, no. 5, pp. 3081–3090, 2014.
[8] A. Thaduri, M. Aljumaili, R. Kour, and R. Karim, "Cybersecurity for eMaintenance in railway infrastructure: risks and consequences," *Int. J. Syst. Assurance Eng. Manage.*, vol. 10, no. 2, pp. 149–159, 2019.
[9] CENELEC, "EN 50126 Railway applications–The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," Standard CENELEC EN 50126, European Committee for Electrotechnical Standardization, 2018.
[10] "Functional safety of electrical/electronic/programmable electronic safety-related systems," Standard IEC 61508, International Electrotechnical Commission, Apr. 2010.
[11] K. Hansen, "Security attack analysis of safety systems," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom. (ETFA)*, pp. 1–4, IEEE, 2009.

[12] J. Grønbæk, T. K. Madsen, and H. P. Schwefel, "Safe wireless communication solution for driver machine interface for train control systems," in *Proc. 3rd Int. Conf. Syst. (ICONS)*, pp. 208–213, IEEE, Apr. 2008.

[13] L. J. Valdivia, I. Adin, S. Arrizabalaga, J. Añorga, and J. Mendizabal, "Cybersecurity–The forgotten issue in railways: security can be woven into safety designs," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 48–55, 2018.

[14] Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS)–A risk management methodology," *Commun. Transp. Res.*, vol. 2, 2022. Art. no. 100078.

[15] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, 2019. Art. no. 101660.

[16] M. Kiviharju, C. Lassfolk, S. Rikkonen, and H. Kari, "A cryptographic and key management glance at cybersecurity challenges of the future european railway system," in *Proc. 14th Int. Conf. Cyber Conflict: Keep Moving! (CyCon)*, vol. 700, pp. 265–284, IEEE, 2022.

[17] M. Niland, "Virus disrupts train signals," *CBS News*, Aug. 21 2003. https://www.cbsnews.com/news/virus-disrupts-train-signals/.

[18] W. G. Temple, Y. Li, B. A. N. Tran, Y. Liu, and B. Chen, "Railway system failure scenario analysis," in *Proc. Int. Conf. Crit. Inf. Infras- tructures Secur.*, pp. 213–225, Springer, 2016.

[19] K. Zetter, "Hackers breached railway network, disrupted service," *WIRED*, Jan. 24 2012. https://www.wired.com/2012/01/railyway-hack/.

[20] Koramis GmbH, "Projekt HoneyTrain: Aufbau, Durchführung und Ergebnisse [in German]," White Paper, Koramis GmbH, Saarbrücken, Germany, 2015.

[21] F. A. Scherschel, "Simuliertes Zug-Steuersystem HoneyTrain: 2,7 Millionen Angriffe in sechs Wochen," *heise online*, Sep. 11 2015. https://www.heise.de/security/meldung/Simuliertes-Zug-Steuersystem-HoneyTrain-2-7-Millionen-Angriffe-in-sechs-Wochen-2810967.html.

[22] K. Wilhoit, "KillDisk and BlackEnergy go beyond energy sector," *Trend Micro*, Feb. 11 2016. https://www.trendmicro.com/en_us/research/16/b/killdisk-and-blackenergy-are-not-just-energy-sector-threats.html.

[23] T. Cheshir, "Four cyber attacks on UK railways in a year," *Sky News*, Jul. 12 2016. https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558.

[24] A. Thomas, "Germany's Deutsche Bahn rail operator targeted in global cyberattack," *The Wall Street Journal*, May 13 2007. https://www.wsj.com/articles/germanys-deutsche-bahn-rail-operator-targeted-in-global-cyberattack-1494658493.

[25] S. Gibbs, "Ransomware attack on San Francisco public transit gives everyone a free ride," *The Guardian*, Nov. 28 2016. https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware.

[26] AFP and The Local, "International cyber attacks put ransoms on German rail station screens," *The Local*, May 13 2017. https://www.thelocal.de/20170513/international-cyber-attacks-put-ransoms-on-german-train-departure-boards.

[27] TASS, "Virus attack targeting Russian Railways localized," *TASS*, May 13 2017. https://tass.com/world/945717.

[28] AP, "The Latest: 29,000 Chinese institutions hit by cyberattack," *The Associated Press*, May 15 2017. https://apnews.com/article/f3bc9c0749624febb3770aa362555317.

[29] The Local, "Swedish transport agencies targeted in cyber attack," *The Local*, Oct. ,12 2017. https://www.thelocal.se/20171012/swedish-transport-agencies-targeted-in-cyber-attack.

[30] Ritzau/The Local, "Cyber attack hits Danish rail network," *The Local*, May 14 2018. https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network/amp.

[31] Sixgill Report, "Hacked Chinese rail control system," *Sixgill*, Mar. 3 2019. https://www.hackread.com/wp-content/uploads/2019/03/Hacked-Chinese-Rail-Control-System.pdf.

[32] CBC, "STM says it refused hackers' $2.8M demand in ransomware attack," *Canadian Broadcasting Corporation News*, Oct. 29 2020. https://www.cbc.ca/news/canada/montreal/stm-refused-to-pay-2-8-million-ransomware-attack-1.5782838.

[33] L. Abrams, "Montreal's STM public transport system hit by ransomware attack," *Bleeping Computer*, Oct. 21 2020. https://www.bleepingcomputer.com/news/security/montreals-stm-public-transport-system-hit-by-ransomware-attack/.

[34] N. Tabak, "Ransomware attack hits short line rail operator OmniTRAX," *FreightWaves*, Jan. 9 2021. https://www.freightwaves.com/news/ransomware-attack-hits-short-line-rail-operator-omnitrax.

[35] C. Cimpanu, "Ransomware attack cripples Vancouver public transportation agency," *ZDNet*, Dec. 4 2020. https://www.zdnet.com/article/ransomware-attack-cripples-vancouver-public-transportation-agency/.

[36] M. Macmahon, P. James, and K. Tindale, "TransLink CEO confirms ransomware hack, says payment info not compromised," *News 1130*, Dec. 3 2020. https://www.citynews1130.com/2020/12/03/translink-suspicious-activity-response/.

[37] S. Boynton and J. Armstrong, "TransLink warns staff hackers accessed personal banking information in cyberattack," *Global News*, Dec. 30 2020. https://globalnews.ca/news/7548761/translink-cyberattack-personal-info/.

[38] Reuters, "Hackers breach Iran rail network, disrupt service," *Reuters*, Jul. 9 2021. https://www.reuters.com/world/middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/.

[39] R. Rocca, "TTC says investigation underway amid ransomware attack," *Global News*, Oct. 29 2021. https://globalnews.ca/news/8337090/ttc-ransomware-attack/.

[40] J. Patton, "TTC cyberattack may have stolen information from up to 25K employees, former employees," *Global News*, Nov. 8 2021. https://globalnews.ca/news/8358094/ttc-cyber-attack-investigation-employee-information/.

[41] Reuters, "Italy's state railway may have been target of cyber attack," *Reuters*, March 2022. https://www.reuters.com/world/us/italys-state-railway-may-have-been-target-cyber-attack-2022-03-23/.

[42] L. Sly, "The Belarusian railway workers who helped thwart Russia's attack on Kyiv," *Washington Post*, March 2022. https://www.washingtonpost.com/world/2022/04/23/ukraine-belarus-railway-saboteurs-russia/.

[43] R. Kour, A. Patwardhan, A. Thaduri, and R. Karim, "A review on cybersecurity in railways," *Proc. Inst. Mech. Eng., F, J. Rail Rapid Transit*, 2022.

[44] CENELEC, "EN 50159 Railway applications–Communication, signalling and processing systems–Safety-related communication in transmission systems," standard, European Committee for Electrotechnical Standardization, 2010.

[45] ISA/IEC, "Security for Industrial Automation and Control Systems," Standard ISA/IEC 62443, International Society of Automation & International Electrotechnical Commission, Jul. 2009.

[46] "Code for Design of Subway," National Standard, Ministry of Construction, People's Republic of China, Standard GB 50157-2003, May 2003.

[47] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2nd ed., 2008.

[48] "Operations Control Centers," Standard APTA RT-OP-S-005-03, American Public Transportation Association, Jul. 2018. 3rd revision.

[49] C. Lévy-Bencheton and E. Darra, "Cyber security and resilience of intelligent public transport: Good practices and recommendations," tech. rep., European Union Agency for Cybersecurity (ENISA), Attiki, Greece, Dec. 2015.

[50] J. Pachl, *Railway Signalling Principles*. Braunschweig, Germany, 2 ed., October 2021. doi: 10.24355/dbbs.084-202110181429-0.

[51] A. Fantechi, "Connected or autonomous trains?," in *Proc. Int. Conf. Rel., Saf., Secur. Railway Syst. (RSSRail)*, (Cham, Switzerland), pp. 3–19, Springer, 2019.

[52] "Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements," Standard IEEE 1474.1, The Institute of Electrical and Electronics Engineers, Feb. 2005.

[53] M. Ghazel, "A control scheme for automatic level crossings under the ERTMS/ETCS level 2/3 operation," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2667–2680, 2017.

[54] M. Schenker, "S2R Innovation Days Presentation X2R3-TD2. 8 Virtually Coupled Train Sets," in *Shift2Rail Innovation Days*, (Brussels, Belgium: European Union), 2020.
[55] "FFFIS for Eurobalise," Standard SUBSET-036, UNISIG, 2012.
[56] J. Mikulski, *Management Perspective for Transport Telematics: 18th International Conference on Transport System Telematics, TST 2018, Krakow, Poland, March 20-23, 2018, Selected Papers*, vol. 897. Cham, Switzerland: Springer, 2018.
[57] UIC–Rail System Department, *FRMCS and 5G for rail: challenges, achievements and opportunities.* International Union of Railways (UIC), Paris, France, Dec. 2020.
[58] "TErrestrial Trunked RAdio (TETRA)." ETSI, Sophia Antipolis, France, 2011.
[59] J. Moreno, J. M. Riera, L. De Haro, and C. Rodriguez, "A survey on future railway radio communications services: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 62–68, 2015.
[60] T. Chothia, M. Ordean, J. De Ruiter, and R. J. Thomas, "An attack against message authentication in the ERTMS train to trackside communication protocols," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, pp. 743–756, 2017.
[61] R. Bloomfield, R. Bloomfield, I. Gashi, and R. Stroud, "How secure is ERTMS?," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.*, (Berlin, Germany), pp. 247–258, Springer, 2012.
[62] J. de Ruiter, R. J. Thomas, and T. Chothia, "A formal security analysis of ERTMS train to trackside protocols," in *Proc. Int. Conf. Rel., Saf., Secur. Railway Syst.*, (Cham, Switzerland), pp. 53–68, Springer, 2016.
[63] L.-j. Chen, Z.-y. Shan, T. Tang, and H.-j. Liu, "Performance analysis and verification of safety communication protocol in train control system," *Comput. Standards Interfaces*, vol. 33, no. 5, pp. 505–518, 2011.
[64] ISO/IEC, "Information technology–Security techniques–Evaluation criteria for IT security–Part 1: Introduction and general model," standard iso/iec 15408-1:2009, International Organization for Standardization (ISO) & International Electrotechnical Commission, Dec. 2009.
[65] ISO/IEC, "Information technology–Security techniques–Information security management systems–Requirements," Standard ISO/IEC 27001, International Organization for Standardization, Oct. 2013.
[66] M. Barrett, "Framework for improving critical infrastructure cybersecurity," NIST Cybersecur. Framework, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Apr. 2018. ver. 1.1.
[67] P. Herzog, "The open-source security testing methodology manual," tech. rep., Inst. Secur. Open Methodol. (ISECOM), Dec. 2010.
[68] ENISA, "Mapping of OES security requirements to specific sectors." European Union Agency for Cybersecurity, Dec. 2017.
[69] UK DfT, *Rail cyber security: guidance to industry.* UK Department for Transport (DfT), London, UK, 2016.
[70] UIC–Rail System Department, *Guidelines for cyber-security in railway.* International Union of Railways (UIC), Paris, France, 2018.
[71] M. Antoni and N. Ammad, "Argus project-harnessing asset management to do cyber security to an uic guideline for railways," in *Congrès Lambda Mu 21 ≪Maîtrise des risques et transformation numérique: opportunités et menaces≫*, 2018.
[72] R. Bloomfield, M. Bendele, P. Bishop, R. Stroud, and S. Tonks, "The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned," in *Proc. Int. Conf. Rel., Saf., Secur. Railway Syst. (RSSRail)*, (Cham, Switzerland), pp. 3–19, Springer, 2016.
[73] É. Masson and C. Gransart in *Proc. Int. Workshop Commun. Technol. Vehicles (Nets4Cars/Nets4Trains/Nets4Aircraft)*, (Cham, Switzerland), pp. 97–104, Springer.
[74] "4SECURail." https://www.4securail.eu/.
[75] L. Alexe, H. Pereira, P. Ribeiro, M.-H. Bonneau, and F. Marqués, "Safety and security requirements of rail transport system in multi-stakeholder environments," deliverable d2.1, CYbersecurity in the RAILway sector (CYRai) EU Project 730843, 2017.
[76] "X2Rail." https://cordis.europa.eu/project/id/730640.
[77] "Roll2Rail." http://www.roll2rail.eu/.
[78] "Safe4RAIL." https://safe4rail-1.safe4rail.eu/.
[79] M. Rekik, C. Gransart, and M. Berbineau, "Cyber-physical security risk assessment for train control and monitoring systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, pp. 1–9, IEEE, 2018.
[80] NIST Joint Task Force, "Security and privacy controls for information systems and organizations," NIST Special Publication 800-53, National Institute of Standards and Technology, Gaithersburg, MD, USA, Sep. 2020. Rev. 5.
[81] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security," NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, MD, USA, May 2015. Rev. 2.
[82] CENELEC, "Railway applications–Cybersecurity," standard ts 50701:2021, European Committee for Electrotechnical Standardization, Jul. 2021.
[83] C. Schlehuber and S. Benoliel, "CENELEC prTS 50701 (Railway applications – CyberSecurity)," in *Proc. Cybersecurity Railways*, pp. 1–18, ENISA-ERA, 2021.
[84] C. Schlehuber, M. Heinrich, T. Vateva-Gurova, S. Katzenbeisser, and N. Suri, "Challenges and approaches in securing safety-relevant railway signalling," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, pp. 139–145, 2017.
[85] J. Warsinske, M. Graff, K. Henry, C. Hoover, B. Malisow, S. Murphy, C. P. Oakes, G. Pajari, J. T. Parker, D. Seidl, and M. Vasquez, *The Official (ISC)^2 Guide to the CISSP CBK Reference.* Hoboken, NJ, USA: Wiley, 5 ed., May 2019.
[86] "Common Vulnerabilities and Exposures (CVE)." https://cve.mitre.org/.
[87] D. Basile, M. H. ter Beek, and V. Ciancia, "Statistical model checking of a moving block railway signalling scenario with Uppaal SMC," in *Leveraging Applications of Formal Methods, Verification and Validation (ISoLA)* (T. Margaria and B. Steffen, eds.), vol. 11245 of *Lecture Notes in Computer Science*, (Cham, Switzerland), pp. 372–391, Springer, 2018.
[88] E. Russo, G. Costa, and A. Armando, "Scenario design and validation for next generation cyber ranges," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, pp. 1–4, IEEE, 2018.
[89] H. Winter, "System security assessment using a cyber range," in *Proc. 7th IET Int. Conf. Syst. Saf., Incorporating Cyber Secur. Conf.*, pp. 1–5, IET, 2012.
[90] T. Gustafsson and J. Almroth, "Cyber range automation overview with a case study of CRATE," in *Proc. Nordic Conf. Secure IT Syst.*, pp. 192–209, Springer, 2020.
[91] E. Russo, G. Costa, and A. Armando, "Building next generation Cyber Ranges with CRACK," *Comput. Secur.*, vol. 95, 2020. Art. no. 101837.
[92] G. Costa, E. Russo, and A. Armando, "Automating the generation of cyber range virtual scenarios with VSDL," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 13, pp. 61–80, December 2022.
[93] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, 2015.
[94] G. Berra, G. Ferraro, M. Fornero, N. Maunero, P. Prinetto, and G. Roascio, "PAIDEUSIS: A remote hybrid cyber range for hardware, network, and IoT security training," in *Italian Conf. Cybersecurity (ITASEC)*, pp. 284–297, 2021.
[95] "Ansible." https://www.ansible.com/.
[96] "Cisco Modeling Labs (CML)." https://developer.cisco.com/modeling-labs/.
[97] "Common Open Research Emulator (CORE)." https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/CORE/.
[98] "Emulated Virtual Environment - Next Generation (EVE-NG)." https://www.eve-ng.net/.
[99] "Graphical Network Simulator 3 (GNS3)." https://www.gns3.com/.
[100] "Mininet." http://mininet.org/.
[101] L. D. Ghein, *MPLS Fundamentals.* San Jose, CA, USA: Cisco, 2016.
[102] Cisco Systems, "MPLS in the DCN," 2007. https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/telco_dcn/Book/telco5.html.

[103] Cisco Systems, "Configuring a Basic MPLS VPN," 2020. https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html.
[104] S.-Y. Chang, S. Cai, H. Seo, and Y.-C. Hu, "Key update at train stations: Two-layer dynamic key update scheme for secure train communications," *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, pp. 125–143, 2016.
[105] V. Dolk, D. P. Borgers, and W. Heemels, "Output-based and decentralized dynamic event-triggered control with guaranteed Lp-gain performance and Zeno-freeness," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 34–49, 2016.
[106] B. Gao, B. Bu, W. Zhang, and X. Li, "An intrusion detection method based on machine learning and state observer for train-ground communication systems," *IEEE Trans. Intell. Transp. Syst.*, 2021.
[107] R. J. Thomas, M. Ordean, T. Chothia, and J. De Ruiter, "TRAKS: A universal key management scheme for ERTMS," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, pp. 327–338, 2017.
[108] L. Zhu, H. Liang, H. Wang, B. Ning, and T. Tang, "Joint security and train control design in blockchain-empowered CBTC system," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8119–8129, 2021.
[109] K. B. Vekaria, P. Calyam, S. Wang, R. Payyavula, M. Rockey, and N. Ahmed, "Cyber range for research-inspired learning of "attack defense by pretense" principle and practice," *IEEE Trans. Learn. Technol.*, vol. 14, no. 3, pp. 322–337, 2021.
[110] M. H. ter Beek, A. Legay, A. Lluch Lafuente, and A. Vandin, "Quantitative security risk modeling and analysis with RisQFLan," *Comput. Secur.*, vol. 109, p. 102381, 2021.
[111] M. E. Kuhl, M. Sudit, J. Kistner, and K. Costantini, "Cyber attack modeling and simulation for network security analysis," in *Proc. Winter Simul. Conf.*, pp. 1180–1188, 2007.
[112] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Comput. Secur.*, vol. 88, p. 101636, 2020.
[113] "CyberChallenge.IT." https://cyberchallenge.it/.
[114] UIC–Passenger Department, *High Speed Rail–Fast Track to Sustainable Mobility*. International Union of Railways (UIC), Paris, France, May 2018.
[115] M. Garmendia, C. Ribalaygua, and J. M. Ureña, "High speed rail: implication for cities," *Cities*, vol. 29, pp. S26–S31, 2012.
[116] UIC–Communication Department, *A global vision for railway development*. International Union of Railways (UIC), Paris, France, Nov. 2015.
[117] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proc. Workshop New Secur. Paradigms*, pp. 71–79, 1998.
[118] B. Schneier, "Attack trees," *Dr. Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.
[119] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC)*, pp. 186–198, Springer, 2005.
[120] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. Weippl, "Dark clouds on the horizon: Using cloud storage as attack vector and online slack space," in *Proc. USENIX Secur. Symp.*, pp. 1–11, 2011.
[121] P. K. Manadhata and J. M. Wing, "An attack surface metric," *EEE Trans. Softw. Eng.*, vol. 37, no. 3, pp. 371–386, 2010.
[122] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Tech. Rep. ADA586960, DTIC, Fort Belvoir, VA, USA, 2013.
[123] V. Drake, "Threat Modeling." https://owasp.org/www-community/Threat_Modeling.
[124] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in *IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, pp. 69–76, IEEE, 2016.
[125] G. Pizzi, "Cybersecurity and its integration with safety for transport systems: Not a formal fulfillment but an actual commitment," *Transp. Res. Proc.*, vol. 45, pp. 250–257, 2020.
[126] R. Kour, A. Thaduri, and R. Karim, "Railway defender kill chain to predict and detect cyber-attacks," *J. Cyber Secur. Mobility*, pp. 47–90, 2020.
[127] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE J. Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.
[128] W. Duo, M. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," *IEEE J. Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.
[129] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *J. Syst. Softw.*, vol. 149, pp. 174–216, 2019.
[130] K. J. Higgins, "How lockheed martin's "kill chain" stopped securid attack," *Dark Reading*, 2013. https://www.darkreading.com/attacks-breaches/how-lockheed-martin-s-kill-chain-stopped-securid-attack.
[131] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," white paper, SANS Institute, Rockville, MD, USA, October 2015.
[132] R. Albach, P. Didier, and H. Dahir, "IoT and Industrial Security Deep Dive. Recommendations and Best Practices," in *Cisco live! (#CLUS)*, Cisco, 2019. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECIOT-2300.pdf.
[133] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare and Security Research* (J. Ryan, ed.), vol. 1, pp. 80–106, New York, NY, USA: Academic, 2011.

Simone Soderi (Senior Member, IEEE) received the M.Sc. degree from the University of Florence, Italy, in 2002, and the Dr.Sc. degree from the University of Oulu, Finland, in 2016. Currently, he is an Assistant Professor with the IMT School for Advanced Studies Lucca. He has published journals and conference papers and chapters in a book. He holds five patents on wireless communications and positioning. His skills range from cybersecurity and wireless communications to software engineering. His research interests include cybersecurity for critical infrastructure systems, 6G, covert channels, network security, physical layer security, electromagnetic emissions security, VLC, and UWB.

Daniele Masti was born in Siena, Italy, in 1993. He received the bachelor's degree in computer and information engineering from the University of Siena, Italy, in 2015, the master's degree in electric and automation engineering from the University of Florence, Italy, in 2018, and the Ph.D. degree in systems science from the IMT School for Advanced Studies Lucca, Italy, in 2021. Since 2022, he has been a Researcher of cyber security with the IMT School for Advanced Studies Lucca. His research interests include the border between control theory and machine learning, with the overall aim of bridging the gap between the two, and network security.

Yuriy Zacchia Lun (Member, IEEE) received the M.Eng. degree in telecommunications engineering from the University of L'Aquila, L'Aquila, Italy, in 2012, and the joint Ph.D. degree in computer science from the Gran Sasso Science Institute (GSSI) and the IMT School for Advanced Studies Lucca, Italy, in 2017. He has been a Visiting Ph.D. Student with the OXCAV Group, Department of Computer Science, University of Oxford, and a Research Collaborator with the University of L'Aquila and IMT Lucca. He is currently an Assistant Professor with the University of L'Aquila. His research interests include the automatic control of wireless networked control systems; communication, computation, and control co-design; and stochastic hybrid systems, formal methods, and cyber-physical security. For more information: zacchialun.com