




Aria Mirzai, Ramana Reddy Avula, Marvin Damschen

## Cybersecurity Risk Assessment of Virtually Coupled Train Sets

### Zoom Authors

	<p><b>Aria Mirzai</b> holds a M.Sc.Eng. degree in Automation and Mechatronics, as well as a M.Sc. in High-Performance Computer Systems from Chalmers University of Technology in Gothenburg, Sweden. Currently, he serves as a researcher at RISE Research Institutes of Sweden, focusing on ensuring the safety and cybersecurity of reliable and autonomous systems. In the Europe’s Rail project R2DATO, Aria investigates the implementation of IEC 62443 compliance in railway systems, primarily for risk assessment. In addition to his contributions to research projects, Aria also holds cybersecurity courses and oversees the institute’s early-stage researchers network.  <a href="mailto:aria.mirzai@ri.se">aria.mirzai@ri.se</a></p>
	<p><b>Ramana Reddy Avula</b> received the B. Tech. and M. Tech. degrees in electrical engineering from the Indian Institute of Technology, Madras, India, in 2015, and the Ph.D. degree in electrical engineering from the KTH Royal Institute of Technology, Sweden, in 2023. From 2015 to 2017, he was a Senior Engineer with Robert Bosch Engineering and Business Solutions, India, where he contributed to the development of sensor signal processing applications for automotive vehicle safety. Currently, he is a Researcher with the Department of Electrification and Reliability, RISE Research Institutes of Sweden. His research interest lies in statistical signal processing with a primary emphasis on enhancing the safety, security, and reliability of autonomous and semi-autonomous vehicles.  <a href="mailto:ramana.reddy.avula@ri.se">ramana.reddy.avula@ri.se</a></p>
	<p><b>Marvin Damschen</b> is a senior researcher with a Ph.D. in Computer Science from the Karlsruhe Institute of Technology, Germany (2018). At RISE Research Institutes of Sweden, he leads EU and national projects, managing teams and substantial budgets. His expertise centers on the digitalization and automation of transport sectors, focusing on railway systems and mobile machinery. He has contributed to European railway advancements through the Shift2Rail project X2Rail-3 and the EU Rail project R2DATO, developing technologies to enhance the efficiency and safety of rail systems. He is also the creator of WayWise, a library for rapid prototyping of connected, autonomous vehicles, developed at RISE Dependable Transport Systems.  <a href="mailto:marvin.damschen@ri.se">marvin.damschen@ri.se</a></p>

## Introduction

In recent years, the increasing digitalisation and interconnectedness of railway systems have underscored the critical importance of robust cybersecurity measures. Notable cybersecurity incidents, such as the sabotage of more than 20 trains in Poland via simple "radio-stop" commands using low-cost equipment [1], highlight the vulnerability of these complex systems to disruptions that can have far-reaching consequences. Moreover, the evolving threat landscape, characterised by increasingly sophisticated ransomware and distributed denial-of-service (DDoS) attacks, poses ongoing challenges that demand continuous vigilance and adaptation [2]. The regulatory response, including stringent EU directives such as the Cybersecurity Act and the NIS 2 Directive, reflects a concerted effort to elevate the cybersecurity standards that impact the transportation sector.

The objective of this work is to provide a cybersecurity risk assessment of the Virtually Coupled Train Set (VCTS) design that is developed within the R2DATO EU Rail project [3]. This work leverages the methodologies developed under the Shift2Rail (S2R) initiative, particularly the X2Rail-5 project [4]. The assessment aims to identify potential vulnerabilities and assess the impact of potential threats. Risk and target security level evaluations for VCTS are presented for identifying applicable security requirements from IEC 62443. By applying a risk assessment tool based on IEC 62443-3-2 and CLC/TS 50701 [5] [6] towards regulatory compliance measures, this work seeks to fortify the cybersecurity of railway systems, ensuring safer and more reliable operations in an increasingly digital landscape.

## Background

### Virtually Coupled Train Sets (VCTS)

VCTS represents an innovative advancement in rail transportation that enables multiple train consists to operate closely together in a coordinated manner without the need for physical coupling. This system promises significant improvements in railway capacity, energy efficiency, and operational flexibility. The virtual coupling concept has been developed within the X2RAIL-3 project [7], which produced detailed operational and functional architectures of the VCTS. Further development is currently underway in the R2DATO project, which aims to advance the VCTS architecture with detailed design of internal and external interfaces with other subsystems.

### Cybersecurity Risk Assessment

The X2Rail-5 method employs the Microsoft STRIDE threat model [8], which categorises threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The method estimates the likelihood of these threats materialising by evaluating several factors: threat type, attacker capability, intent, and targeting. The Common Vulnerability Scoring System (CVSS) exploitability metrics further refine this likelihood assessment.

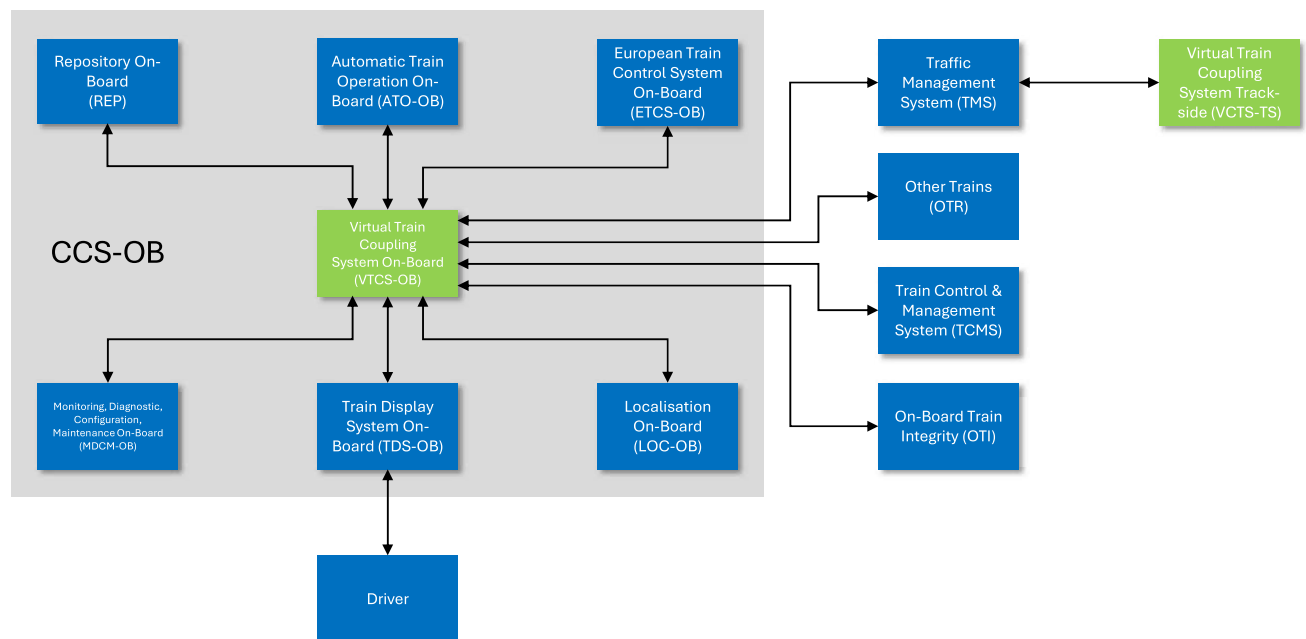
Compared to other methodologies, e.g., developed by EULYNX RCA OCORA [9], the X2Rail-5 methods specifically targets compliance with IEC 62443-3-2, which addresses security risk assessment for system design [6]. Further, the method is supported by a publicly available Excel-based risk assessment tool that guides implementing cybersecurity measures in accordance with IEC 62443 (part 62443-3-2 in particular), covering both IEC 62443-3-2 and IEC 62443-4-2 requirements.

## System description

Today's railway architecture is the result of many decades of incremental, component-wise transformations, making it inflexible, challenging to integrate, and costly to upgrade or replace. Additionally, there is no unified EU perspective on a common future railway system architecture, as individual railway systems maintain distinct national or regional technical approaches. This makes it challenging to design, analyse, and integrate innovative solutions like VCTS, which have interfaces with other subsystems. To address this challenge, Europe's Rail Joint Undertaking established a System Pillar (SP) consortium. This consortium aims to ensure

that the evolution of the rail system is based on common operational visions and a layered functional architecture. At the time of writing, there are no architectural outputs from the SP. However, expert discussions indicate that the SP architecture of the onboard Control Command and Signalling (CCS) subsystem is expected to align with the Open CCS On-board Reference Architecture (OCORA) [10]. Consequently, in this work, OCORA is considered as a technological baseline for the signalling system architecture.

By integrating the VCTS architecture developed in X2RAIL-3 with OCORA [11], we present a simplified block diagram of the system under consideration (SuC) showing its interfaces with other subsystems in Figure 1. According to this, we divide the SuC into two security zones (SZ) as shown in Table 1. As this work is based on a system architecture which is subject to change, and since the communication channels for VCTS are expected to be provided by the existing train network and other ETCS components such as Euroradio, risk assessment of the conduits is omitted. The cybersecurity risk analysis in this work specifically focuses on VCTS system and its components.



**Figure 1:** Simplified block diagram of the system under consideration showing its interfaces with other subsystems.

SZ-name	SZ-ID
VCTS Onboard	OB-Z
VCTS Trackside	TS-Z

**Table 1:** Security Zone classification of the SuC

The VCTS system missions from [12], as shown in Figure 2, are considered as the primary assets (PAs), which are the essential functions of the SuC. At the level of detail of subsystems from Figure 1, the identified list of supporting assets (SAs) that the primary assets depend on are listed in Table 1. VCTS-OB is a required SA for all the analysed PAs, while VCTS-TS is only required for a few. After assessing risk levels using these primary and supporting assets, cybersecurity requirements from IEC 62443-3-3 and IEC 62443-4-2 should be allocated to the security zones (and conduits) of the SuC.

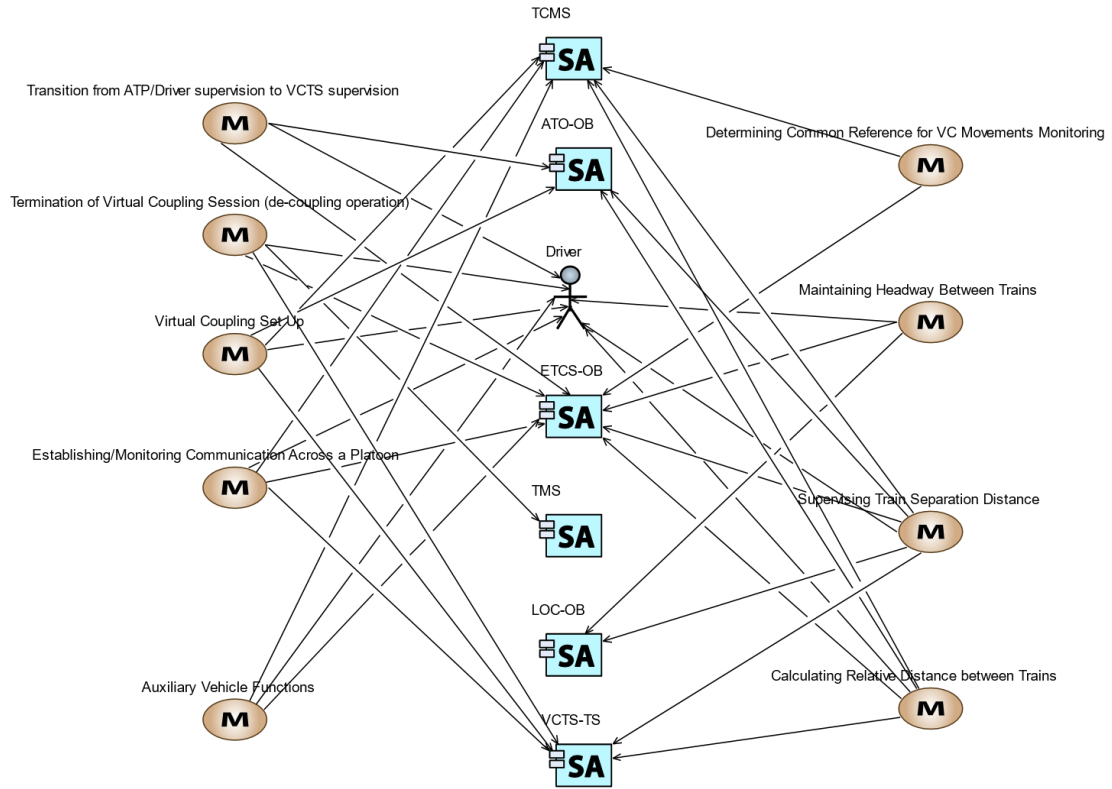


Figure 2: VCTS mission diagram [7]

SA-Title	SA-ID	SA Type	Security Zone
VCTS-Onboard	VCTS-OB	Software Applications	OB-Z
VCTS-Trackside	VCTS-TS	Software Applications	TS-Z

Table 2: VCTS supporting assets

## Cybersecurity Risk Analysis

As the first step, the “Initial Risk Assessment” is performed for each primary asset. This entails evaluation of the impact of each feared event, an excerpt of our results for the primary asset “Virtual Coupling Set Up” is provided in Table 3. The evaluations were performed in two separate pairs for each primary asset with experts from RISE, DLR, Renfe, Indra and CEIT. To consolidate the results, the worst-case evaluation of each business stake (Safety, Performance, Reputation, Compliance) was chosen.

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Total Damage Potential	Overall Impact	Rationale
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	112	2	- Safety: No loss of life, no injuries. - Performance: Train might need to be replaced after the trip. - Reputation: Adverse local/regional media reports. - Compliance: Major non-compliance with contract and regulation.
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	1300	4	- Safety: Major loss of life. - Performance: Major area blocked, or main infrastructure blocked during >1 week. - Reputation: Extensive national media reports. - Compliance: Extensive non-compliance with contract.
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	1210	4	- Safety: Major loss of life. - Performance: Major area blocked, or main infrastructure blocked during >1 week. - Reputation: Extensive national media reports. - Compliance: Extensive non-compliance with contract.

Table 3: VCTS Initial Risk Assessment (excerpt)

## Unmitigated Risk Analysis

The initial risk assessment is followed by a more detailed, so-called “Unmitigated Risk Analysis”. While the former focused on the assessment of impact, the unmitigated risk analysis proceeds by evaluating the likelihood parameter. The first step is the analysis of the Event Initiation Likelihood (EIL), where the X2Rail-5 D11.1 method examines nine types of threat actors capable of triggering threats in the railway domain.

We have reassessed these likelihood criteria for each threat actor, with regards to the current SuC – VCTS. The results are presented in **Table 4**. There are some notable changes in these results compared to the Automatic Train Operation (ATO) Grade of Automation (GoA) 3/4 example presented in X2Rail-5 [5] worth mentioning:

- For VCTS, “Competitors” were considered to possess higher capability, while intent and targeting were simultaneously lowered. One motivation for this being that while competitors in this sector possess extensive knowledge, they are unlikely to attack each other.
- “Terrorist” increased in intent, a motivation for this is that they likely possess a high motivation to enforce their ideological beliefs.
- Government Organisation increased in targeting. An explanation is that this threat actor is the one considered to possess the most resources.
- “Script Kiddy” received a lower targeting, as this actor is unlikely to conduct advanced reconnaissance.

Together with assigned weights, the Excel tool utilises the capability, intent and targeting values to calculate an EIL value for that threat actor.

Weights/Multiplicative Factor			Consideration factor of threat actor <i>(if an actor is not relevant please use "0" for the specific threat actor)</i>									
CAP	INT	TARG	1	1	1	1	1	1	1	1	1	
1	2	3	Event Initiation Likelihood (EIL)									
			Hacker/Cracker	Terrorist	Competitor	Government Organization	Hacktivist	Criminal Organization	Script Kiddy	Layman	Insider	Max EIL
			EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL	EIL
			3	3,83	2,67	3,17	3	4	2	1,5	3,67	4
Delta value (δ)	1	Pessimistic EIL	3,000									
		Balanced EIL	2,98									
		Optimistic EIL	2									

**Table 4** VCTS Event Initiation Likelihood

After the EIL analysis, a vulnerability rationale and CVSS score is derived for each supporting asset. Table 5 shows the VCTS-OB supporting asset only, as an excerpt of our results. The CVSS Score is normalised as “Unmitigated Vulnerability Severity” (UVS). Together with the EIL, it comprises the Overall Unmitigated Likelihood as follows:

$$\text{Overall Unmitigated Likelihood} = \left\lfloor \frac{\text{UVS} \times \text{EIL}}{\text{Max EIL}} \right\rfloor$$

The vulnerability rationale used to derive the CVSS vector is inherited from the X2Rail-5 method but repurposed for this report. However, due to ongoing work on short-range communication for VCTS, they potentially need to be revised in the future. For the context of this work, it is assumed that TCMS handles this type of communication.

SA-ID	STRIDE Threat Category	Vulnerability Rationale	CVSS Vector	CVSS Score	UVS	EIL	Overall Unmitigated Likelihood
VCTS-OB	Spoofing Identity	Attacker can access VCTS-OB and spoof identity via ETCS or TCMS network + remote access interface (e.g. SSH)	AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H	8.9	3	3	2
VCTS-OB	Tampering with data	Attacker can access VCTS-OB and tamper the data via ETCS or TCMS network + remote access interface (e.g. SSH)	AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H	8.9	3	3	2
VCTS-OB	Repudiation	Attacker can access VCTS-OB and delete or modify security log or monitoring service via ETCS or TCMS network + remote access interface (e.g. SSH)	AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N	7.3	3	3	2
VCTS-OB	Information disclosure	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	3.5	1	3	1
VCTS-OB	Denial of Service	Attacker can access VCTS-OB and steal or collect information via ETCS or TCMS network + remote access interface (e.g. SSH)	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.5	2	3	1
VCTS-OB	Elevation of Privilege	Attacker can access the VCTS-OB via ETCS or TCMS network and gain more privileges	AV:A/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:H	7.9	3	3	2

**Table 5:** VCTS Overall Unmitigated Likelihood (excerpt)

In the following, the Overall Unmitigated Likelihood is used to calculate the Unmitigated Risk value. As **Table 6** shows, this value represents the threat influence of each supporting asset on their corresponding primary assets (only results for primary asset Virtual Coupling Set Up and supporting asset VCTS-OB presented here).

Unmitigated Risk is the multiplication of Impact and Overall Unmitigated Likelihood. It is a critical parameter for determining target security level (SL-T) and later allocating security requirements from IEC 62443 for securing the system against the identified risk. Further, we have identified MITRE threats each supporting asset, in accordance with the threat landscape (see Table 47 in [5] for more details), giving a better understanding of potential threats.

Primary Asset	Supporting Asset	STRIDE Threat Category	Vulnerability Type	Impact of Losing	Impact	Overall Unmitigated Likelihood	Unmitigated Risk
PA-01 Virtual Coupling Set Up	VCTS-OB	Spoofing Identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS]	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING]	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS]	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Information Disclosure	[DISCLOSING INFORMATION FROM SOFTWARE APPLICATIONS]	Confidentiality	2	1	2

PA-01 Virtual Coupling Set Up	VCTS-OB	Denial of Service	[DoS Software Applications]	Availability	4	1	4
PA-01 Virtual Coupling Set Up	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS]	Confidentiality	2	2	4

**Table 6:** VCTS Unmitigated Risk (excerpt)

As shown in Table 7, the second but last step in this method is to identify the maximum unmitigated risk by STRIDE domain and security zone.

Max Risk per Zone	S	T	R	I	D	E
OB-Z	8	8	8	4	4	8
TS-Z	8	8	8	4	4	8

**Table 7:** Max Risk per Zone and STRIDE domain

The STRIDE domains are hereafter mapped to the seven foundational requirements of IEC 62443 to identify appropriate requirements for achieving a specific target security level. Each risk level also corresponds to a specific target security level (SL-T).

	IAC	UC	SI	DC	RDF	TRE	RA	SL-T Vector
OB-Z	2	2	2	2	2	2	1	{2, 2, 2, 2, 2, 2, 1}
TS-Z	2	2	2	2	2	2	1	{2, 2, 2, 2, 2, 2, 1}

**Table 8:** Max SL-T per Zone and IEC 62443 FR

Using the SL-T vector, organisations can identify and allocate requirements from IEC 62443-3-3 (for zone/system level) and IEC 62443-4-2 (for component/supporting asset level) to address cybersecurity risks.

## Conclusion & Future Directions

This work presents a cybersecurity risk assessment of Virtually Coupled Train Sets (VCTS) within the R2DATO EU Rail project, leveraging methodologies from the Shift2Rail project X2Rail-5 and aligning with IEC 62443 standards. The analysis identifies critical vulnerabilities and evaluates potential threats using the Microsoft STRIDE threat model and CVSS exploitability metrics, demonstrating the effectiveness of a structured approach to cybersecurity within railway.

The Excel tool provided by X2Rail-5 is compliant with IEC 62443-3-2 and ISA/IEC 62443-4-2 and provides practical guidance for enhancing cybersecurity in railway systems. Key findings in its application highlight the importance of continuous improvement in risk assessment methodologies and the need for a detailed vulnerability severity analysis.

Future enhancements could involve more specific guidelines and examples, such as leveraging attack trees and MITRE attack techniques to generate vulnerability vectors more precisely tailored to the system in focus, and broader asset types, including information assets and processes. Also, aligning the threat landscape in [5] with the Transport Threat Landscape for the European Union made by ENISA [2] would greatly increase its legitimacy. This work advances cybersecurity in railway systems, providing a foundation for future research and development to ensure safer and more reliable operations in a digital and interconnected world.

## References

- [1] A. Greenberg, "The Cheap Radio Hack That Disrupted Poland's Railway System," WIRED, 27 August 2023. [Online]. Available: <https://www.wired.com/story/poland-train-radio-stop-attack/>. [Accessed 3 July 2024].
- [2] European Union Agency for Cybersecurity, ENISA threat landscape 2023: July 2022 to June 2023, Publications Office of the European Union, 2023.
- [3] "Rail to Digital automated up to autonomous train operation: FP2 - R2DATO Project," [Online]. Available: <https://cordis.europa.eu/project/id/101102001>. [Accessed 3 July 2024].
- [4] "Completion of activities for Adaptable Communication, Moving Block, Fail safe Train Localisation (including satellite), Zero on site Testing, Formal Methods and Cyber Security: X2Rail-5 Project," [Online]. Available: <https://cordis.europa.eu/project/id/101014520>. [Accessed 3 July 2024].
- [5] X2RAIL-5, "Deliverable D11.1 Cybersecurity assessment of other TD's," Shift2Rail, 2023.
- [6] X2RAIL-5, "Deliverable D14.3 Support of the Europe's Rail SP with Cyber Security Topics," Shift2Rail, 2024.
- [7] X2Rail-3, "Deliverable D6.1 Virtual Train Coupling System Concept and Application Conditions," Shift2Rail, 2020.
- [8] Microsoft Corporation, "The STRIDE Threat Model," 2005. [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)). [Accessed 3 July 2024].
- [9] EULYNX/RCA and OCORA, "(Cyber) Security Guideline (Version: 1.00)," RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2021.
- [10] OCORA, "Introduction to OCORA, OCORA-BWS03-010, Version: 6.20," OCORA Cooperation, 2023.
- [11] OCORA, "CCS On-Board (CCS-OB) Architecture, OCORA-TWS01-035, Version: 4.00," OCORA Cooperation, 2023.
- [12] X2RAIL3, "Deliverable D7.5 Business Model," Shift2Rail, 2021.