Rail to Digital automated up to autonomous train operation

D48.2 – Virtually Coupled Train Set conceptual studies (VCTS): use case definition and operational concept analysis

Due date of deliverable: 31/05/2025

Actual submission date: 17/04/2025

Leader/Responsible of this Deliverable: Kevin Mullankuzhy, DLR

Reviewed: Y

Document status		
Revision	Date	Description
01	15/04/2025	Workpackage 48 review included
02	04/07/2025	TMT review included
03	30/01/2026	SP, EU-Rail - external expert review included.

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	PU

Start date: 01/12/2022 Duration: 42 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union's Horizon Europe research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Kevin Mullankuzhy	DLR	Chapters 3.3, 5.1.2, 5.2 and reviewer
Riccardo Parise	DLR	Chapters 5.1.2 and 5.2
Paul Unterhuber	DLR	Reviewer and inputs from T48.4
Daniel Lüdicke	DLR	Chapters 4.2, 4.3 and review Chapter 6
Michael Roth	DLR	Chapter 4.1
Marvin Damschen	RISE	Chapters 3.4, Chapter 6 and reviewer
Aria Mirzai	RISE	Chapters 3.4, Chapter 6 and reviewer
Ramana Reddy Avula	RISE	Chapters 3.4, Chapter 6 and reviewer
Anders Lindfeldt	TRV/KTH	Reviewer
Francisco Parilla Ayuso	INDRA	Chapters 3.1, 5.1.1 and review of Chapter 4.2 and 4.3.
Paula Diaz Serrano	INDRA	Chapters 3.1, 5.1.1 and review of Chapter 4.2 and 4.3.
Björn Uhrig	SMO	Chapter 3.2 and review of Chapter 4.1
Diego Garcia Vaquero	Renfe	Reviewer
Francisco Haro Fortes	Renfe	Reviewer
Rodrigue Fargeon	SNCF	Reviewer

Disclaimer

EXECUTIVE SUMMARY

The railway sector is undergoing significant transformation to meet increasing demand while addressing infrastructure limitations. The Virtually Coupled Train Set (VCTS) is an innovative operational solution with the potential to transform railway operations by increasing capacity, efficiency, flexibility, and interoperability while paving the way for higher levels of automation. However, with the rapidly evolving railway sector and ongoing modernization efforts, introducing disruptive operational concepts such as VCTS presents challenges.

Deliverable D48.2, "Virtually Coupled Train Set (VCTS) Conceptual Studies: Use Case Definition and Operational Concept Analysis," explores innovative solutions to enhance railway capacity and operational efficiency within Europe's Rail framework. The objective of this deliverable is to analyze the current operational and technological baselines of railways, describe how VCTS fits into the ecosystem, identify relevant use cases for VCTS implementation, highlight key aspects critical for its development, and provide strategic recommendations to various stakeholders.

To define the state of the art and advancements in the railway sector, the study surveyed several predecessor projects, standards, and railway initiatives investigating enabling technologies for VCTS. Prior research and technological developments in VCTS from 2018 to 2023 were systematically reviewed, incorporating insights from Connecta-1, 2 and 3, X2Rail-3, SCOTT, MovingRail, and INSECTT. The study identified four primary use cases—mainline freight, mainline passenger, low-density networks, and urban mass transit—each with distinct operational challenges and stakeholder implications.

A technological baseline was defined by aligning VCTS with the latest publicly available and technically developed (although not yet finalised) reference architectures available at the time of drafting this deliverable in November 2023, which offer more advanced possibilities for integrating emerging technologies than the existing ERTMS/ETCS specifications, namely, RCA – Baseline 1 Release 0 (trackside systems) and OCORA – Release 4 (onboard systems). It is important to note that this deliverable predates the subsequent architecture specification releases by the System Pillar (SP), including the Traffic Control and Supervision (CS) System Concept [1] and the Train CS Baseline 1 [2]. Future VCTS developments should be aligned with the evolving SP architecture, which will require further analysis beyond the scope of this document.

The deliverable also assesses enabling technologies required for VCTS, such as localization and communication technologies, emphasizing a shift toward onboard systems to reduce trackside dependencies. The necessity of the Future Railway Mobile Communication System (FRMCS) for VCTS implementation is highlighted, while legacy systems like Eurobalises and Global System for Mobile Communications (GSM-R) are considered for degraded operational scenarios.

To identify VCTS interfaces and map communication paths, complex architecture models were analyzed. A model-based systems engineering (MBSE) approach was employed to analyze data streams, providing recommendations for VCTS communication requirements.

The operational concept of VCTS is also explored in detail. The layered decision framework defined in predecessor projects is further developed. Various exemplary railway service scenarios in Spain are used to demonstrate how the VCTS operational concept can support different functional goals, such as reducing energy consumption, increasing throughput, or adhering to a timetable. Furthermore, numerical models are used to characterize different VCTS manoeuvre and analyze performance, driving strategies, and interactions between consists of a VCTS.

The cybersecurity risks associated with the VCTS system are also analyzed in this deliverable. Cybersecurity workshops and surveys with experts and partners were conducted to identify threats and risks in VCTS operations. The results of these workshops were used to conduct risk assessments following methodologies from X2Rail-5, ensuring compliance with IEC 62443 and TS 50701 standards. Security vulnerabilities were analyzed and recommendations were provided to mitigate risks.

Deliverable D48.2 makes a significant contribution to the advancement of VCTS within Europe's Rail framework. By addressing system design, operational strategies, and cybersecurity, it lays a solid foundation for future developments in virtual coupling and its potential to transform railway operations.

ABBREVIATIONS AND ACRONYMS

- ABDS – Absolute Braking Distance
- AE – ATO Execution
- AoC – Area of Control
- ASTP – Advanced Safe Train Positioning
- AT – ATO Transactor / ATO Translation
- ATO – Automatic Train Operation
- ATP – Automatic Train Protection
- ATS – Automatic Train Supervisor
- AUG – Augmentation System for Positioning
- CAM – Cooperative Awareness Messages
- CBTC – Communication-Based Train Control
- CCS – Command, Control and Signalling
- CIA Triad – Confidentiality, Integrity, Availability
- CMD – Cold Movement Detection
- DAC – Digital Automatic Coupling
- DDW – Diagnostic Data Writing
- DLR – German Aerospace Center
- DR – Digital Register
- ECN – Ethernet Consist Network
- EDR-OB – ETP Data Recording On-Board
- EGNOS – European Geostationary Navigation Overlay Service
- EKF – Extended Kalman Filter
- EMUS – Electric Multiple Units
- ENISA – European Union Agency for Cybersecurity
- EoA – End of Authority

- EREP-OB – ETP Repository On-Board
- ERA – European Union Agency for Railways
- ERJU – Europe's Rail Joint Undertaking
- ERTMS – European Rail Traffic Management System
- ESA – European Space Agency
- ETCS – European Train Control System
- ETB – Ethernet Train Backbone
- EU-Rail – Europe's Rail Joint Undertaking
- EUG – ERTMS Users Group
- EUSPA – European Union Agency for the Space Programme
- FOT – Fixed Object Transactor
- FRMCS – Future Railway Mobile Communication System
- G2T – Ground-to-Train
- GCG – Ground Communication Gateway
- GNSS – Global Navigation Satellite System
- GPS – Global Positioning System
- GSA – European Global Navigation Satellite System Agency
- HLA – High-Level Architecture
- HUA – Human Actors
- IMU – Inertial Measurement Unit
- IMUS – Inertial Measurement Units
- IPM-ISM – Incident and Prevention Management – Incident Solving Manager
- IRA – Initial Risk Assessment
- ISO – International Organization for Standardization
- JDW – Juridical Data Writing
- JTC – Joint Technical Committee

- KF – Kalman Filter
- KMAC-OB – KMAC Services On-Board
- LC – Level Crossing
- LOC-OB – ASTP as LOC-OB variant in the R2DATO context
- LS – Light Signal
- LWG – Localisation Working Group
- MaaS – Mobility-as-a-Service
- MCG – Mobile Communication Gateway
- MCTS – Mechanically Coupled Train Set
- ME – Maintenance Equipment
- MEMS – Micro-Electro-Mechanical Systems
- MHE – Moving Horizon Estimation
- MITRE – MITRE Corporation (Cybersecurity Framework)
- MOL – Mobile Object Locator
- MOT – Mobile Object Transactor
- MP – Movement Permission
- MT – Movement Authority Transactor
- OA – Object Aggregation
- OCORA – Open CCS Onboard Reference Architecture
- OCS-IM – Operation Control Systems – Infrastructure Manager
- OCS-RU – Operation Control Systems – Railway Undertaking
- OTR – Other Trains
- PAS – Planning and Scheduling System
- PE – Plan Execution
- PETS – Physical ETCS Transponder Service
- PF – Particle Filter

- PK – Kilometer Post (Point Reference)

PRAMSS – Performance, Reliability, Availability, Maintainability, Safety, and Security

- PSL – Person Supervisor & Locator
- PTU-OS – Physical Train Unit Operation Systems
- R2DATO – Rail to Digital Automated up to Autonomous Train Operation
- RAMS – Reliability, Availability, Maintainability, Safety
- RBC – Radio Block Centre
- RBD – Relative Braking Distance
- SAMC – Smart Adaptation Movement Control
- SBAS – Satellite Based Augmentation Systems
- SERA - Single European Railway Area
- SIL – Safety Integrity Level
- SL – Safety Logic
- SLAM – Simultaneous Localization and Mapping
- SM – Safety Manager
- SMC – Sliding Mode Controller
- SRC – Short Range Communication
- SRAS – Smart Rail Automation System
- STCC – Smart Train Composition Coupling
- STR – Status Reports
- SuC – System under Consideration
- T2G – Train-to-Ground
- T2T – Train-to-Train
- TCS – Trackside Condition Services
- TCN – Train Communication Network
- TCMS – Train Control and Management System

- TDS – Train Detection System
- TDS-OB – Train Display System On-Board
- TIM – Train Integrity Monitoring
- TMS – Traffic Management System
- TMS – Train Management System
- TPR – Train Position Reports
- TRL – Technology Readiness Level
- TS – Time Service for Synchronization
- TS – Track Side
- TSI – Technical Specifications for Interoperability
- UKF – Unscented Kalman Filter
- V2V – Vehicle-to-Vehicle
- VB – Virtual Balise
- VBR – Virtual Balise Reader
- VCTS – Virtually Coupled Train Sets
- VOBC – Vehicle Onboard Controller
- WSN – Wireless Sensor Network
- ZC – Zone Controller

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

2 INTRODUCTION

The present document constitutes the deliverable D48.2 “Virtually Coupled Train Set conceptual studies (VCTS): use case definition and operational concept analysis” in the framework of Task 48.2 of the WP48 contributing to TE11 “Virtually Coupled Train Sets (VCTS)”. WP48 deals with innovative operational solutions, which are currently under lower TRL.

Task 48.2 also has strong links to Task 48.4. Task 48.2 focuses on the conceptual studies and theoretical foundations of VCTS, while task 48.4 addresses the key technical enablers for the implementation of VCTS which are Short-Range Communication (SRC) and Relative Localisation (RL).

Deliverable D48.2 builds upon the VCTS concept developed in predecessor projects CONNECTA-2 and X2Rail-3, aiming to

- Define the VCTS concept within Europe’s Rail.
- Identify and list use cases for VCTS.
- Define system design and interfacing based on state of art technologies and reference architectures.
- Propose VCTS driving strategies informed by models and numerical simulations.
- Assess cybersecurity risks of VCTS.

The shift from road to rail transport is accelerating. However, existing bottlenecks in the Trans-European Network indicate that rail infrastructure is nearing its capacity limits. Constructing new railway lines is both costly and environmentally challenging. Thus, optimizing the capacity of the existing rail network is a more viable solution.

Technologies such as ETCS Level 2 and ETCS Level 2 Moving Block are already enhancing railway efficiency and capacity. VCTS takes this a step further by leveraging train-to-train communication and onboard sensor technologies to enable virtual coupling. This approach reduces the minimum distance between trains by allowing independent trains to form virtually coupled platoons, increasing operational flexibility and throughput, shortening coupling times, and improving the robustness of railway operations.

VCTS has been researched in several predecessor projects in Euope’s Rail. This deliverable builds upon these projects. Chapter 3 defines the state of the art of VCTS concept based on these predecessor projects. It reviews and summarizes insight from various projects dealing with VCTS concepts such as X2RAIL-3, CONNECTA, MOVINGRAIL, SCOTT and InSecTT and summarizes the highlights. It also outlines 4 possible use cases that were identified for VCTS.

Chapter 3 also describes the operational and technological baselines, including how VCTS fits into the most consolidated reference architectures available at the time of drafting this deliverable in November 2023—namely, RCA – Baseline 1 Release 0 (trackside systems) and OCORA – Release 4 (onboard systems). It presents the functional architecture of VCTS along with its required building blocks. Since the completion of this deliverable task, the SP has released new architecture specifications: Traffic CS System Concept (trackside) and the Train CS Baseline 1 (onboard). A brief summary of these recent developments, along with a high-level comparison to the RCA and OCORA baselines, is also included in this chapter.

Chapter 4 defines the VCTS system and the required interfaces. It discusses the current state of various localization technologies relevant to VCTS, including those researched under R2DATO, such as RL and SRC (developed in Task 48.4), ASTP (developed in WP21 and WP22), Digital Register (DR) (developed in WP27), and OTI (developed in WP19 and WP20). Furthermore, the chapter discusses train-to-train and train-to-ground communication concepts and their respective interfaces. Additionally, a data stream analysis is conducted using an MBSE Capella model, refined from X2Rail-3.

Chapter 5 examines VCTS operational concepts through various models and simulations. It evaluates different tactics and driving strategies under varying scenarios to illustrate the practical implementation of the VCTS concept.

Finally, Chapter 6 presents a detailed cybersecurity risk assessment of VCTS. It outlines the methodology used and summarizes the results of the threat and risk analysis workshop conducted with project partners in Gothenburg in 2024.

3 DEFINITION OF THE VCTS CONCEPT WITHIN EUROPE'S RAIL

3.1 SUMMARY OF THE VCTS CONCEPT FROM THE PREDECESSOR PROJECTS

The current shift towards urban living has resulted in a changing mobility landscape, with fewer city dwellers relying on cars and a growing demand for efficient, modern, timely and environmentally friendly transport options. This trend has notably driven an increase in demand for rail transportation [3].

To deal with this increased demand, it is necessary to expand rail lines or upgrade existing ones. Building new lines is often costly, consequently, the focus has been on optimizing existing infrastructure. Recognizing the varied and fluctuating demand for rail travel throughout the day and year, a flexible mode of transport with high-capacity passenger trains and modular train compositions has been deemed necessary. The modern commuter trains are usually "Electric Multiple Units", EMUs, which has been designed as modular based on the following ideas:

- Can be coupled with other EMUs, but usually only with other EMUs of their same train series.
- Passenger cars can be added or subtracted (the train can become longer or shorter), but this operation is time costly and not easy (particularly when the passenger cars share bogies between them).

To face these challenges, the rail industry has concentrated on improving current operations. Research efforts have focused on, among many other things, increasing capacity by reducing intervals between trains.
Conventional train protection systems are based on the **absolute braking distance** of trains, operating under, first fixed block principles and then moving on to moving block principles [4]. These are the two most common philosophies currently applied across Europe and worldwide.

- **Fixed blocks** are applied in most national signalling systems. They divide the track into different sections, so that train movements are only allowed up to the entry point of the next occupied section. This solution does not maximise the railway capacity, as it is mainly limited by the fact that once one train enters a track section, the whole section becomes unavailable for other trains. So, trains using absolute stopping distance principles must set their stopping target (End of Authority – EoA) at the beginning of the occupied track section.

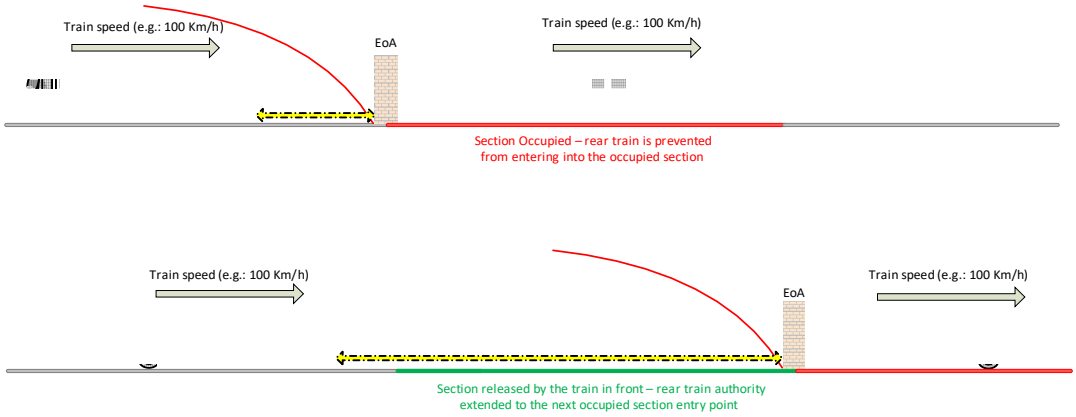

Figure 1: Fixed Block Approach **[4]**

- **Moving blocks**, which thanks to absolute safe train positioning and train integrity system that report data continuously, can reduce the distance between trains. ERTMS 2 Moving Block (formerly known as ERTMS Level 3) and CBTC are good examples of this. In this way it is not necessary to: adjust the EoA of the following trains and define an entry point to a section (an association is made directly to the rear end of the train in front).
  In this instance as well, the monitoring of braking curves proves inefficient, as it assumes that the trailing train must have the capability to come to a complete stop before reaching the present position of the leading train, irrespective of the leading train's current velocity and braking curve.

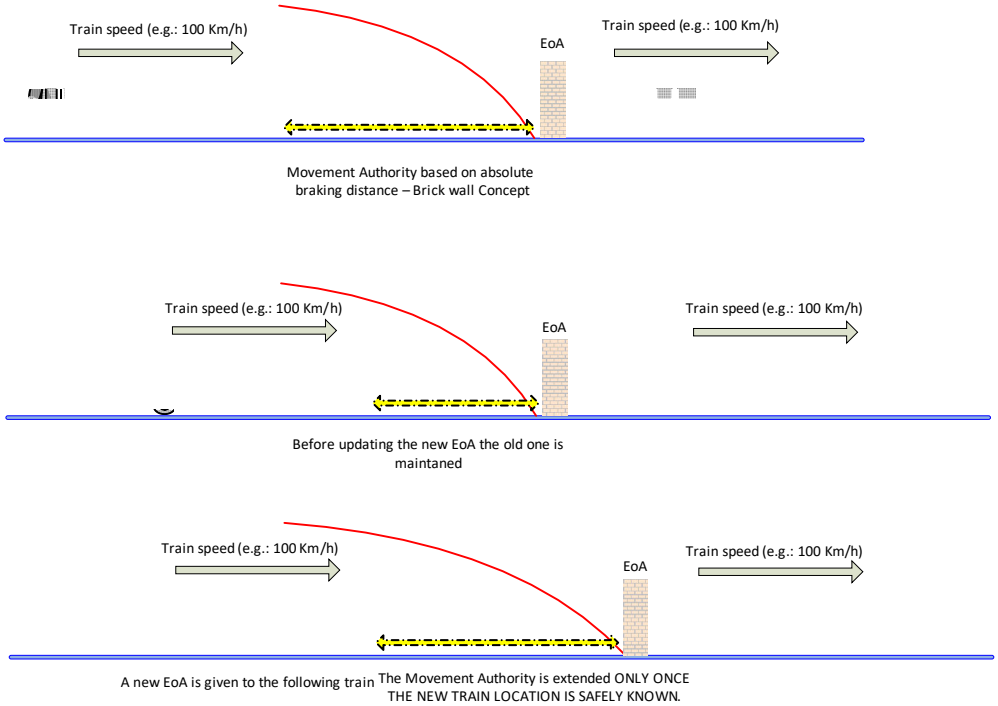

Figure 2: Moving Block Approach **[4]**

One of the main challenges facing this modernization is the increase in of railway capacity while maintaining the safety. Therefore, it is important to review the **European Train Control System (ETCS)** concept. ETCS has the following levels [5]:

- Level 1: at this level, conventional signalling systems based on fixed blocks, defined by the distance between fixed signals on the track, are used. This means that trains must maintain predefined safety distances, which reduces operational flexibility and limits the capacity of the railway line.
  To ensure the safety and supervision of train movement, Eurobalises installed at strategic points on the railway infrastructure, are used. These balises provide Automatic Train Protection (ATP) information intermittently, allowing speed monitoring and applying automatic braking in case the set limits are exceeded.
  Communication between the track and the train is one-way, meaning that the balises transmit information to the train, but the train cannot send data back to the infrastructure. In addition, the information provided at discrete locations and not in real time, which implies less precise monitoring of the train's status and position on the track. This operating model reduces the efficiency of the railway system and restricts its ability to adapt to dynamic traffic conditions.

Additionally, emergency braking is activated only when the train reaches a checkpoint with programmed beacons, which can lead to inefficiencies in incident management.

- Level 2 Fixed Block: introduces a significant improvement by implementing a two-way communication system between the train and the infrastructure, known as Train-to-Ground (T2G) and Ground-to-Train (G2T) communication. GSM-R is currently used as the main T2G/G2T communication (ERTMS implementation), although in the future a transition to FRMCS is planned for more efficient and robust communication.
  Thanks to the continuous and uninterrupted communication between the track and the train (T2G/G2T), information flows in both directions: the railway infrastructure sends data to the train about the track status, speed limits and traffic conditions, while the train transmits its position, speed and operational status in real time. This allows for better traffic regulation and greater responsiveness to unforeseen events.
  One of the key advantages of Level 2 is the complete elimination of line side signalling, as all relevant information is transmitted directly to the trains via the Radio Block Centre (RBC) system. However, train detection still relies on the division into fixed blocks, determined by track circuits and axle counters. Although the distance between blocks can be adjusted to improve adaptability and increase track capacity, it is still subject to certain restrictions inherent to the fixed block model. The train receives Movement Authority (MA) information, which tells it how far it can advance, depending on the state of rail traffic on its route.

- Level 2 Moving Block (Formerly known as ETCS level 3): It represents a radical evolution in railway management, as it eliminates both fixed track signals and track circuits, adopting a new paradigm based on moving blocks. In this model, the safety distance between trains is dynamically adjusted based on their speed, trajectory and operating conditions, allowing for more efficient circulation and greater line capacity, but always considering ABD.
  Communication with trains remains based on GSM-R, with a future transition to FRMCS for better reliability and lower latency.
  At this level, train detection no longer depends on track circuits or axle counters, but is based mostly on self-location of trains using on-board sensors, such as GNSS (Global Navigation Satellite System) systems and integrated odometry. The elimination of fixed detection infrastructure allows for larger flexibility and cost reduction in railway infrastructure.

  In practice, Level 2 Moving Block has evolved into an intermediate concept known as Hybrid Level 2, explored in WP15 and 16, which combines elements of Level 2 with the introduction of Hybrid Train Detection (HTD). This hybrid approach allows for a progressive transition from fixed blocks to mobile blocks, ensuring greater compatibility with existing infrastructure and facilitating the implementation of cutting-edge technologies in railway operation.

Once the minimum distance between trains has been optimized (following ABD), the only option to increase the number of passengers is to increase the capacity of the trains. A **mechanically coupled train set** (MCTS) is a train made up of two or more trains that can also run independently, it is based on the mechanical coupler. This coupler is the device that connects the trains mechanically and serves as a bridge to transfer information between consists [4].

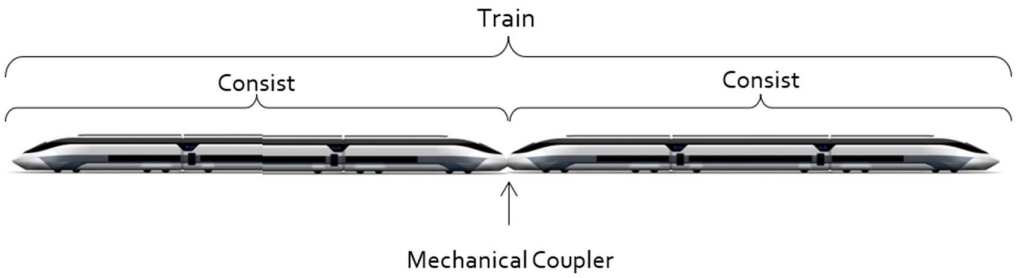

Figure 3: Mechanical Coupling Train Set of two Consist (MCTS) **[4]**

The procedures for coupling and uncoupling mechanically are well established in the railway system. The definition of where and when the consists join and separate is based on their compatibility, destinations and schedules. It should be noted that the coupling being automatic (DAC) or not automatic, implies one technical stop (resulting in extra time and extra energy consumption) and in the manual one (not DAC, nowadays) an operator must couple and lock the mechanical connection,increasing even more the manouvre time. There are several aspects to consider for this procedure to be carried out successfully, it is necessary that the trains involved are compatible in terms of mechanical coupling (or conventional coupling) and technical parameters must be defined to carry out the coupling and uncoupling. Apart of that, it is needed that the trains involved are:

- Electrically coupled (control of traction).
- Pneumatically coupled (braking capabilities).
- Electronically coupled (control of other systems in the coupled train, like lighting, HVAC, etc.).

To build longer sets and overcome all the previous drawbacks, new application principles are promoted to replace the conventional coupling. An innovative idea known as **Virtual Coupling (VC)** emerges. Virtual coupling provides a more evolved system that allows trains to run together as mechanically coupled, but without any physical connection.

To do that, we need to change the paradigm of protection systems based on the **absolute braking distance** of trains to **relative braking distance**.

Virtual coupling allows several trains to circulate on the same line, reducing the separation between them. The trains behave as if they were physically coupled, thanks to wireless **train to train communication**, so that the capacity of the line would be increased to a greater extent than with moving blocks [3] or complementing it. And not only this, but it provides **a more flexible operations** of the line, since it makes possible the circulation of trains in small series, adapting each time to the circumstances. In addition, this solution offers the possibility of reducing costs and allows dynamic route planning, among other benefits.

The ability to perform virtual couplings also provides **greater flexibility** to increase the number of stops and generate new economically viable routes. This adds an additional layer of flexibility to the generation of new routes and planning them in real time, which helps to further optimize the efficiency of the railway system. This not only increases the capacity and efficiency of rail transport, but also promotes greater integration with multimodal transport, thus laying the foundations for a more efficient and sustainable transport system in the future.

Figure 4: Virtual Coupling (VC) **[6]**

As mentioned above, in VC the physical link disappears and is replaced by the virtual link. This implies that the trains in the platoon can have different kinematic behaviours and characteristics at any time. Due to the lack of physical contact, VCTS trains can be coupled and uncoupled in circulation without risk. Many of the limitations that physical coupling brought with it are overcome. VCTS is then based on maintaining a safe distance between trains while allowing the movement of trains as close as possible.

To review the concept of VCTS it is necessary to analyse a series of **relevant projects** where this concept takes on an important value:

Projects	Start date	End date	VC related topic
CONNECTA 1 [7]	September 1, 2016	September 30, 2018	It contributes to the development of Train Control and Monitoring Systems (TCMS) with wireless capabilities, as well as the next generation of electronic braking systems. It focuses on the concept of Train-to-Ground (T2G) communications and how the network of one train extends to that of another identical train.
SCOTT [8]	May 1, 2017	October 31, 2020	This project introduces the concept of VC and works on the specification, design, development, deployment and testing of a complete VC system (with a first implementation of the strategic layer – based on a timetable – and the operational layer).
CONNECTA 2 [9]	October 1, 2018	July 31, 2021	In line with the preceding CONNECTA initiative, the associated works are related to the paradigm of T2G communications.
X2Rail-3 [10]	December 1, 2018	November 30, 2021	The project studies virtual coupling, as a concept that allows trains to circulate much closer to each other and dynamically modify their own composition in motion. The architecture of the VCTS system is technically defined.
MOVINGRAIL [11]	December 1, 2018	December 31, 2020	It focuses on the transition from fixed blocks to moving ones, to obtain train-centric signalling and therefore, among many other aspects, a communications architecture is defined for virtual coupling.
InSecTT [12]	June 1, 2020	August 31, 2023	Provide comprehensive and cost-effective smart, secure and reliable connectivity, and interoperability

			solutions to bridge the Internet of Things and artificial intelligence. The operational layer (Virtual Coupling manoeuvres) is improved through the development of AI modules that provide better fluidity in speed change processes to increase the comfort of passengers and the confidence of transport companies in this type of virtual composition.
CONNECTA 3 [13]	December 1, 2020	July 31, 2023	This project continues the work developed in previous CONNECTA projects, advancing in the preparation of the train monitoring and control system.

Table 1: Relevant projects related to VC.

SCOTT is the first project in which the concept of virtual coupling begins to be conceived as a whole system. It works on the specification, design, development and deployment of a complete Virtual Coupling system. In turn, within the framework of this project, the first virtual coupling test is carried out based on the implementation of the strategic and operational layer.

The SCOTT project [4] seeks a reliable virtual coupling solution for trains. This solution aims to safely execute all the different scenarios, the coupling itself and coupling and uncoupling manoeuvres between sets of trains. The ultimate objective of the work carried out at SCOTT was always to increase the capacity of the line, improve the operation of train compositions in coupling and decoupling, incorporating secure communications between trains.

Starting from the state of the art, SCOTT defines different use cases associated with the main problems detected. These are:

- Train detection
- Report on risk situations
- Coupling/decoupling operation cost
- Interoperability between trains

Based on the analysis of the use cases, in SCOTT worked on launching a first approach for the Virtual Coupling On-Board Unit (VC-OB). The VC-OB as the central unit on the train that, as can be see below, must have at least interfaces with the proximity WSN (wireless sensor networks), the TCMS, the module for T2T communications and the ATP and ATO systems.

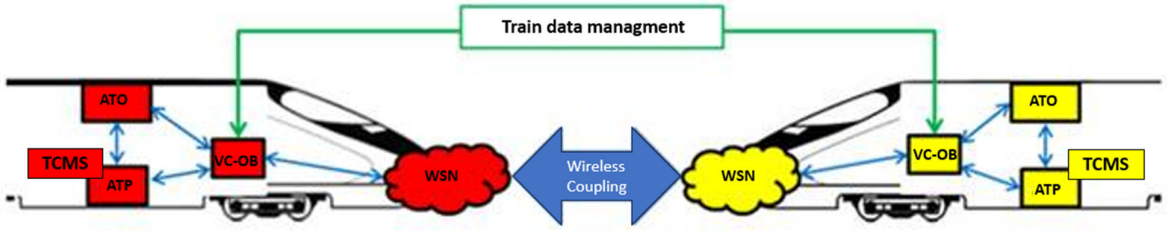

Figure 5: VC-OB Main interfaces. Source: Indra Sistemas S.A.

It is then the following high-level architecture (HLA
) for the smart train composition coupling (STCC) On-Board Unit:

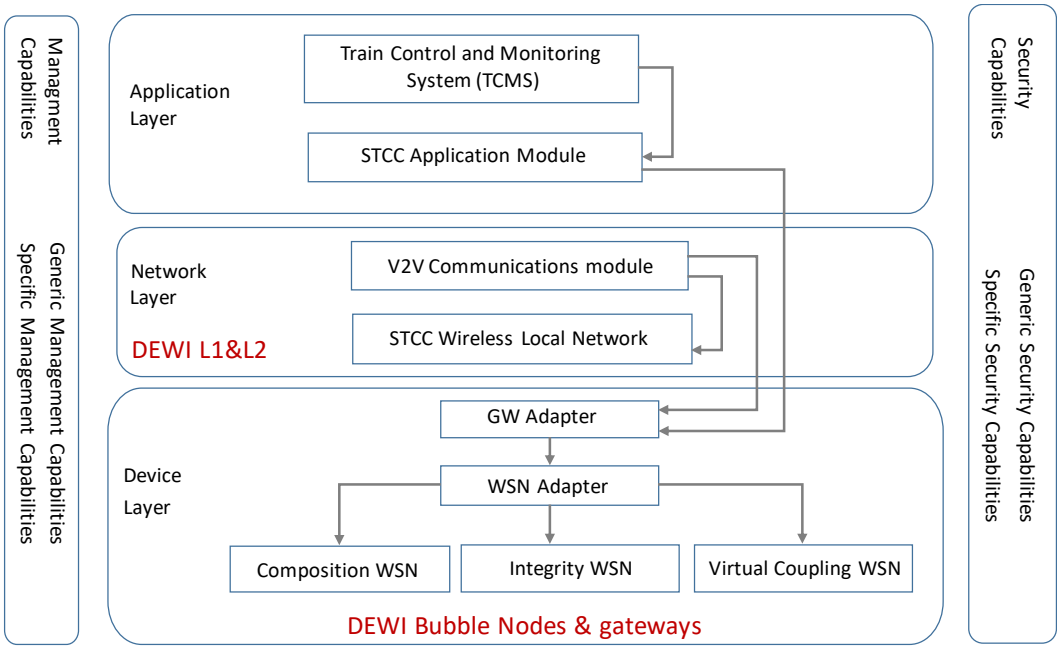

Figure 6: HLA STCC- OB. Source: Indra Sistemas S.A.

Below is the description of each module. Starting with the device layer:

- Virtual Coupling WSN: in this module a WSN capable of measuring the distance between adjacent trains is developed.
- Integrity WSN: this module is responsible for detecting the integrity of the train. In turn, it sends raw data about the integrity of the STCC-OB.
- Composition WSN: system that collects data on the composition of the train (weight, length, etc.) to send them to the STCC-OB

The three mentioned modules are connected directly to the WSN adapter.

- WSN adapter, this module collects all the information from the different WSNs that are connected to it. Functions as an application router managing inputs and outputs, is content independent and addresses security and service output issues (availability, security, timing, etc.).
- GW (gateway) adapter: is the module responsible for receiving data from the WSN adapter and processing it on the STCC Application Module and/or send it directly to the train consists (through the V2V Communication module).

Moving on to the network and application layer, there are the following modules:

- STCC Application module: this module processes the data from the WSNs, TCMS, ATP, ATO, etc and is responsible for: generating movement authorities, movement directives and

all the required signalling messages and managing the safety of the composition and the link created for the virtual coupling.
- V2V Communications module: this module sends the data processed by the STCC application module if the train is the leader and receives processed data in the case in which it is the commanded train.

The Intelligent Train Composition Coupling (STCC) system allows obtaining a unique composition with two or more trains that circulate while maintaining the minimum distance between them. In this way, it is possible to increase the capacity of the line in addition to facilitating the coupling and uncoupling of trains without the need to deploy personnel for the operation.
In turn, virtual coupling would allow trains equipped with the STCC system to share the same line so that not only would it save time, costs and facilitate the operation, but it would also considerably increase the capacity of the line.

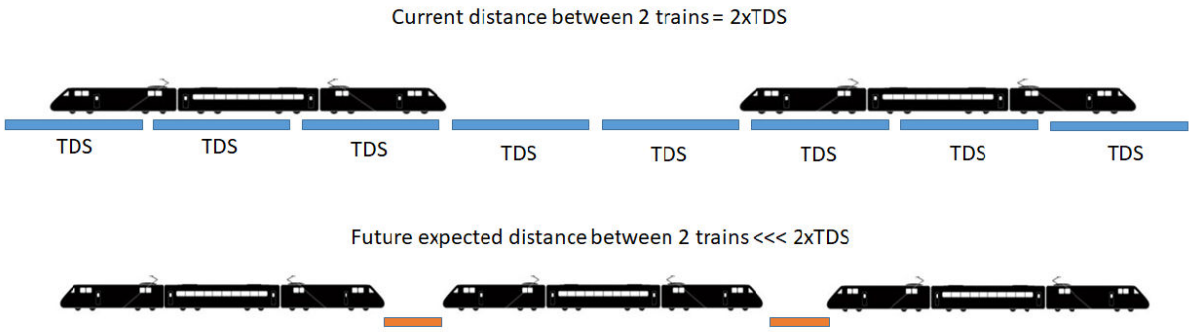

Figure 7: Increasing the capacity of the railway line through the contribution of the STCC system. Source: Indra Sistemas S.A.

In SCOTT the following assumptions are made to generate a first approach (based on Wireless communications SoA and STCC Requirements):

- Three types of specific zones are defined for each operation: the coupling manoeuvre zone, the coupling zone and the uncoupling manoeuvre zone. All this based on railway topology, terrain topography and safety regulations.
- Coupling operation is only acceptable and may be permitted in certain areas, to allow co-existence between strategic layer (basically the planner of the Train Management System (TMS)) and STCC systems.
- Virtual coupling is allowed in areas where a direct signal line between trains can be achieved.
- Following Spanish regulations [14] (as a first reference), it is assumed that two Train Detection Systems (TDS) is the minimum distance allowed so that the compositions managed by the TMS can approach each other.
- The STCC system manages the compositions of both trains, from the moment a T2T communication link is established until the end of the virtual coupling manoeuvre. To do this, the strategic Layer (through the Plan defined in the TMS) and ATP systems must allow it.

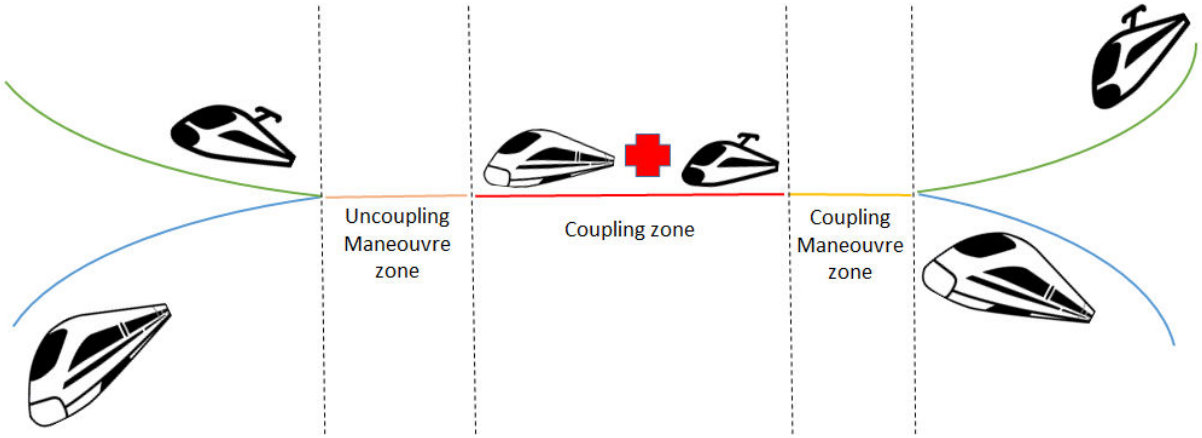

Figure 8: Virtual coupling and uncoupling manoeuvres. Source: Indra Sistemas S.A.

Just as different zones are foreseen, in the first approximation of the STCC system, two different driving modes are foreseen, the coupling/uncoupling manoeuvre mode and the coupling mode (Figure 9).
In the coupling manoeuvre mode, the trains approach each other and in the coupling mode both trains are managed by the lead train.

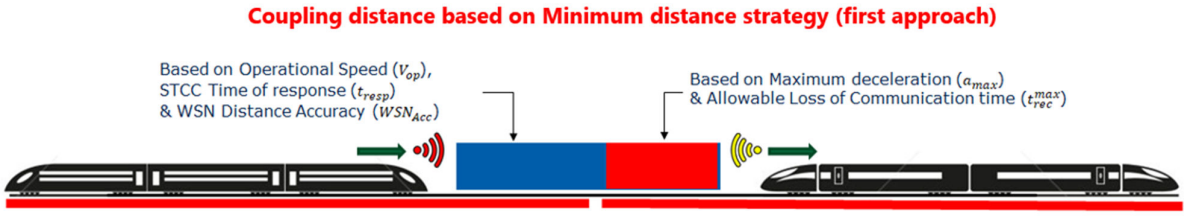

Figure 9: Coupling Mode. Source: Indra Sistemas S.A.

Moving on to analyse the next project, **X2Rail-3** [4], the approach and definition of the VCTS concept are outlined in this project. The entire design effort begins with the identification of a series of fundamental scenarios that outline the main operational landscape and obstacles that the VCTS intends to address. This initial phase is also based on collaborative efforts with other initiatives such as MOVINGRAIL.

From these scenarios, the functional description of VCTS is developed, defining the basic functions, principles, and main objectives. The technical functions of the VCTS address the overall description of the system's precise role and scope within the current infrastructure, as well as establishing the boundaries concerning tasks assigned or requirements delegated to external subsystems. The next step of conceptual design is to detail the functional requirements specifications.

The primary objective guiding the application principles of VCTS is to substitute the traditional mechanical coupling method employed between two or more trains, thereby facilitating the formation of longer train sets. The significance of the VCTS concept lies in its endeavour to supplant the time-intensive mechanical coupling process with a more adaptable and swift approach. This entails introducing a "virtual" coupling mechanism that dispenses with the need for a physical mechanical device to link trains. Instead, it introduces an advanced system enabling trains to operate jointly as if they were mechanically coupled, although without any tangible physical connection.

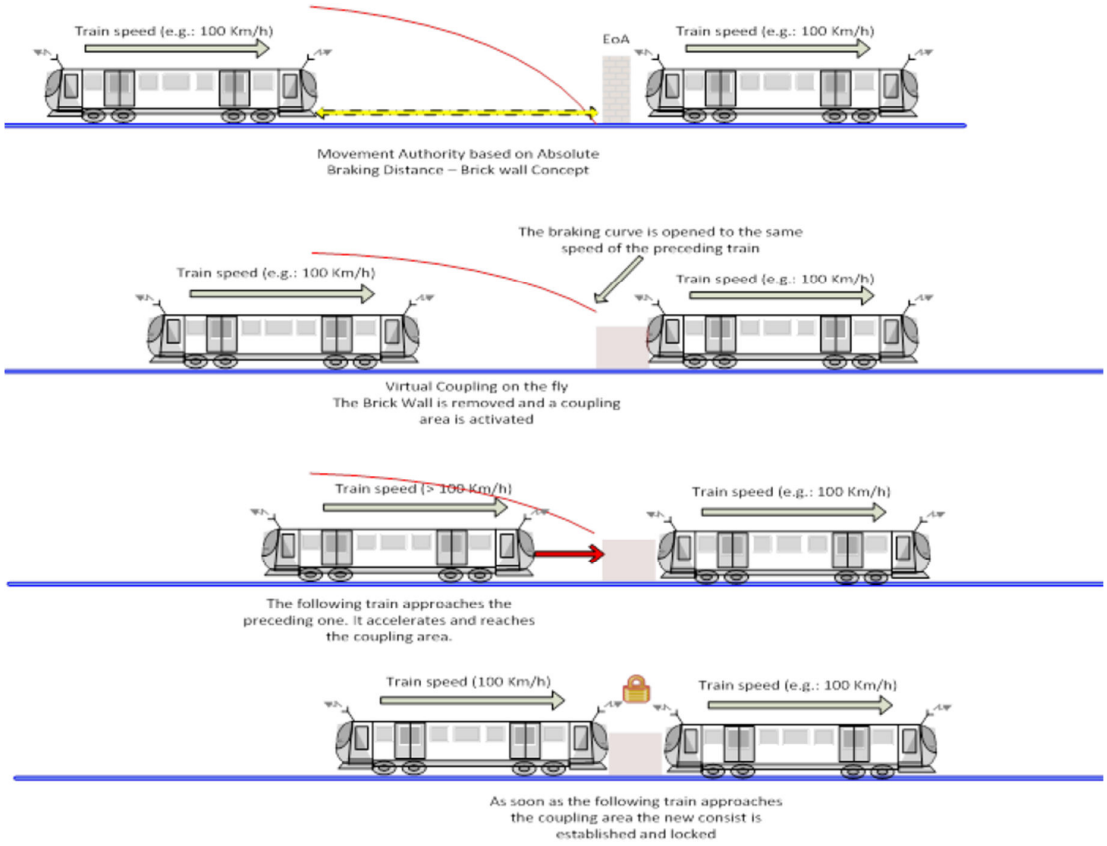

Figure 10: VCTS Conceptual Approach **[4]**

Referring to Figure 10, the concept of operation for VCTS is based around the principle of overcoming the limitation imposed on train progress caused by the application of absolute braking distance. To do this, there must be a mutual exchange of relevant information between two or more trains, so that the train's progress control system allows them to travel at a distance shorter than the absolute braking distance of the second part. In this way, the train can calculate 'cooperative' braking curves, which integrate into its algorithm the parameters related to the braking characteristics and the state of the train within the virtually coupled train, as well as other parameters such as network delay, communication, etc.

As a result, components within the virtually coupled train must be allowed to circulate at a shorter distance than the current absolute braking distance paradigm, to form a VCTS. The core of the VCTS is therefore the ability of components within a platoon to interact via a dedicated communication link to exchange data and allow the virtual coupled train component to implement the forward control strategy.

From the X2Rail-3 project the following functional **layers diagram** is obtained that allows us to have an overview of the system:

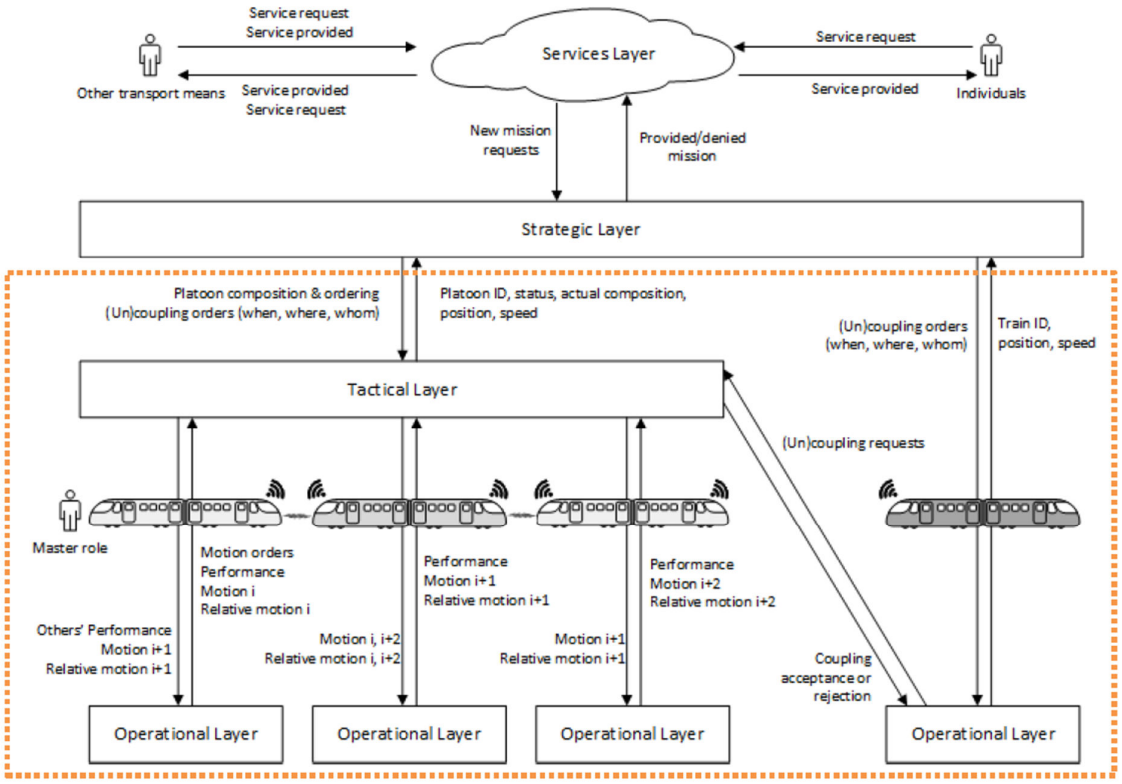

Figure 11: Functional layers and VCTS system **[4]**.

The system that falls within the scope of the X2Rail-3 project is marked in orange, while the VCTS system comprises the entire figure. The VCTS system has been decomposed into four main parts or processes, each of them corresponding to a functional layer:

- **Service layer**: requests new rail services (missions) and is integrated into the mobility-as-a-service (MaaS) platform. It is important to know that it is outside the scope of the VC system, belonging to the service provider.

  This layer is responsible for coordinating the requirements of new services according to demand and interacts with users, who could be individuals accessing railway reservation systems or other transportation mode platforms.
  Additionally, it requests new and ongoing missions from the strategic layer to fulfil the requested services.

- **Strategic layer**: the strategic layer is related to the service layer and the tactical layer. In the strategic layer, the strategy is defined to follow a plan and objectives, what and when are defined. The aim of this layer is to optimize infrastructure capacity, identify potential conflicts, manage delays and disruptions, and oversee traffic flow while ensuring safety measures are upheld. Is in charge of defining the composition and ordering of the platoons, based on compatibility, destinations and schedules. And it defines when and where trains join and leave the platoon.

  From the upper layer there are service requests, from them, an algorithm determines how to create the platoons, whether based on artificial intelligence, machine learning, etc. These platoons are organized in such a way that they always seek to achieve objectives in terms of capacity, punctuality, operating costs, travel time or waiting time, and many others.

In turn, this layer determines when and where the trains join and leave the platoons. To do this, therefore, a permanent communication link must be established between this subsystem and the trains. The procedure is as follows: individual trains report their speed and position and from time to time receive commands regarding virtual coupling procedures (coupling time and place).
At the same time, the identification of the platoon (or master train) is reported on the track side.

This capability of the strategic layer is key to ensure the route-vehicle compatibility (TSI OPE). For example, in the existing infrastructure, it can be found in some stations short platforms that have enough length for a certain long train. If two of those trains are on a platoon, it will be needed to decouple them before entering the station so they can embark/disembark passengers as if they were separated trains.

- **Tactical layer**: the tactical layer is related to the strategic layer and the operational layer. In this layer, what to do to carry out the strategy is defined. Also coordinates the platoon movements and manoeuvres, manages sudden degraded modes of any platoon unit, is responsible of defining the acceleration and speed targets and the headway between trains (is connected to the signalling system).
  The strategic layer should be capable of organizing, managing, and virtually dividing sets of trains in an operationally efficient manner to avoid challenging entry or exit manoeuvres. If necessary, the tactical layer would also be responsible for managing the operation by controlling individual distances within the platoon.

  The Tactical layer coordinates the movement of the trains that make up the platoon from the moment the incorporation request is received until the platoon is dissolved. The procedure is as follows, when a train receives the joining order, contact is established with the target and a dialogue is established to verify the coupling capabilities. This process adheres to the current signalling system (such as ERTMS), which relies on absolute braking distance, until the VCTS assumes control and permits the minimum headway (based on monitoring relative braking distance). Subsequently, the joining train can proceed with the approach following the regulations of virtual coupling.
  Once the platoon is created and the advance occurs, the tactical layer is responsible for the stable movement of the platoon.

- **Operational layer**: the operational layer is related to tactical layer. Oversees the local control of each unit, that is, its acceleration and braking, to ensure that what is established in the tactical layer is executed safely. The main task in terms of control is to regulate the platoon's advance while always maintaining its stability.
  This layer manages the local movement of each train safely following the orders provided by the tactical layer. Therefore, the main function of this layer is to regulate the advance of the platoon, maintaining stability.

  This layer is present locally in each train and is linked to subsystems such as traction and brakes.

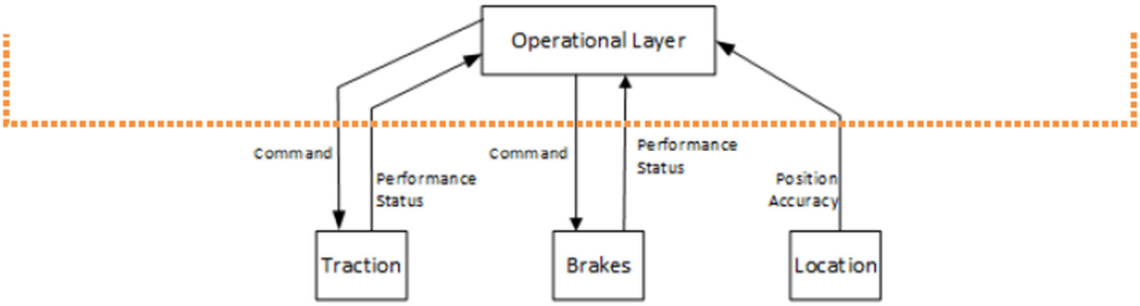

Figure 12: Operational layer and train subsystems relations **[4]**.

The VCTS project in X2Rail-3 proposed the specification of requirements as a basis for future developments and demonstrators, following Model-Based Systems Engineering (MBSE [15]) methodology (ARCADIA [16]) implemented by the **CAPELLA** tool. VCTS is composed of an on-board part (VCTS-OB) and a trackside part (VCTS-TS) [17].
On the specifications, the designed architecture and the development of VC and intelligent track objects obtained as a result in X2Rail-3, and on the results obtained in the first implementation of VC in terms of manoeuvre during the SCOTT project, there is still potential for improvement when trying to prioritize passenger comfort and cargo safety.

The InSecTT project [18] project aimed to continue the development of the operational layer, focus on new technologies (such as Artificial Intelligence) to allocate control resources efficiently and promote innovations in the railway field. From a more technological point of view and focused on virtual coupling, the aim was to implement AI applications to improve virtual coupling and distance adjustment, to increase the comfort and confidence of passengers and cargo, respectively. At the same time, the development of a secure and reliable decentralized decision control system was also sought.
The work done at SCOTT concerning VC, as seen above, while solving the fact of having a secure wireless virtual coupling, doesn't go further in terms of passenger comfort and safe cargo travel, during the coupling mode. Therefore, artificial intelligence is used to:

- Automate the smoothing of coupling and decoupling processes. This automation is achieved by improving the Control, Command and Signalling (CCS) modules of the STCC-OB.
- Improve security at the T2T and T2G communication level.
- Increase line capacity and optimize track occupancy.

The aim is to improve the management of the operation layer, through supervised automatic learning, in order to adjust the parameters of the coupling operations as best as possible to the real dynamic parameters of the trains, smoothing the manoeuvres and making them more comfortable for passengers. Two collaborative system called **Smart Adaptation Movement Control (SAMC)** and **Smart Rail Automation System (SRAS)** are developed to improve the operational layer. These modules provide two sets of functions. One set of functions that relate to optimize the movement directives. And two, a set of functionalities related to the coupling automation [18].

- SAMC: this module is used to smooth the coupling; it is capable of controlling speed changes so that trains can comfortably perform speed variations. Its objective is to perfect the train's movement directives by adapting to the capabilities of the rolling stock.
- SRAS: The trains, according to the travel schedule, will use the Automatic Train Regulation System to coordinate their movements taking into account the real conditions of the areas through which they travel. With the purpose of decentralizing Automatic Train Operation

(ATO), SRAS will implement an Artificial Intelligence algorithm to make decisions regarding the execution of the planned trip.
Additionally, SRAS will make decisions considering rail infrastructure information to determine whether a train has priority in critical areas. Therefore, SRAS will continuously evaluate the railway plan and traffic data, such as train density or the status of railway signals status, to manage train travel conditions.
The AI module will be responsible for facilitating the train formation process, optimally adjusting the spacing between them and obeying SRAS guidelines. In other words, more than one train with different destinations could travel together.

These solutions will contribute to improving the line's capacity, providing greater flexibility and guaranteeing better compliance with schedules thanks to more efficient traffic management. All these operations will be carried out safely, comfortably and in line with road operations. As a result, rail infrastructure will be more adaptable in terms of schedules and accessibility.

Finally, and as a summary, InSecTT adapts the coupling system to the architecture defined in X2Rail-3 and always based on the previous work and research developed in SCOTT, to improve both the operational and tactical layers in the VCTS system.
In parallel to these projects, we cannot lose sight of the contribution of **CONNECTA 1**, **2** and **3**, and **MOVINGRAIL** to the concept of VC.

Referring to the **MOVINGRAIL** project, there is a proposal for the European rail network to implement a system in which the lead train of a platoon receives an ETCS movement authority, while all subsequent trains within the platoon are granted a "Virtual Coupling Movement Authority". This virtual authority allows these trains to be virtually coupled to the leading train.
MOVINGRAIL establishes several criteria for communication systems [19], in turn, a method was established to determine the communication requirements for virtual coupling. Emphasis is placed on the need for direct communication (T2T) beyond the existing requirements of the moving block. The research identified TETRA, Wi-Fi and cellular (5G/3GPP) evolutions as possible communication technologies. After analysing these options, it was concluded that the transition from GSM-R to 5G offers the most promising path for a communication proposal in the European rail network. Furthermore, 5G is considered suitable and economically viable for other sectors, ensuring consistency between various applications.

At the end, in [20] it is proposed that the **communications architecture for virtual coupling is built on the foundations of 5G**.

And finally, making a brief reference to the contribution of **CONNECTA** projects to the VCTS concept in question, we need to talk about the T2G term. The main objective of **CONNECTA 1** [21] is to develop an interoperable T2G communication system. In order to standardize T2G services, **CONNECTA 2** [22] defines a set of requirements for T2G communication protocols and services.
The T2G communication system consists of two parts:

- The on-board mobile communication gateway (MCG), located in the Ethernet Consist Network of a train.
- The ground communication gateway (GCG) located in a ground network.

3.2 DESCRIPTION OF VCTS USE CASES

The use cases in the following subsections try to put the VCTS functionality into its respective context of surrounding subsystems and human actors, assuming an implementation that is making use of the existing ATC systems. The high-level interactions are based on the functional layers from the X2Rail-3 project explained in section 3.1, including the Strategic, the Tactical and the Operational Layers in the system under consideration and excluding the Services Layer as implied there. They deviate per use-case if the overall architecture is assumed to deviate from those functional layers. For each use case the potential gains in performance (in terms of traffic throughput) are provided.

3.2.1 Mainline railways

Mainline passenger railways are increasingly adopting advanced signalling systems to enhance safety and efficiency. The integration of technologies like Moving Block (MB) and Virtual Coupling (VC) is pivotal, as they allow for closer train spacing and reduced headways, thereby increasing line capacity.

3.2.1.1 Mainline Freight Railways

It is assumed that for the VCTS functionality to be available for Mainline Freight Railways

- the wayside installation of the enabling area is a system that follows the ERTMS architecture and includes an RBC and
- the trainborne installation on the involved trains also follows the ERTMS architecture and includes an ATO.

The actors of the Mainline freight railways use-case hence are the following (see Figure 13):

- Strategic Layer
  - Requests missions from the VCTS
  - Receives feedback with denial or permission of a mission
- ATO
  - Derives the Operational Dynamic Speed Profile from the VCTS
- OBU
  - Derives the Vital Dynamic Speed Profile from the VCTS
- Train Driver
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- ATS
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- RBC
  - Derives the VCTS Status
- Neighbour VCTS
  - Establishes the Link
  - Provides Control Data

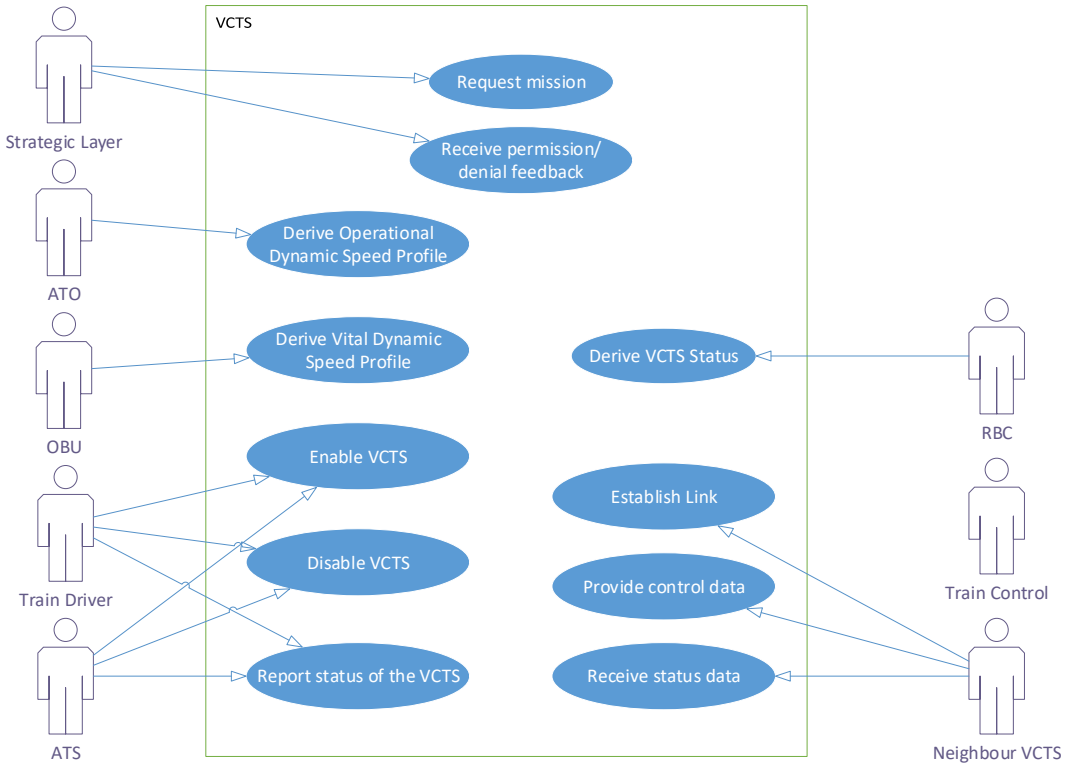

Figure 13: Use Case Diagram for Mainline Freight Railways

The potential performance gains provided by VCTS for Mainline Freight Railways are:

- Reducing headway down to absolute braking distance
- Increasing performance at bottlenecks between junctions (especially for layouts without stations between the junctions)
- Increasing the capacity of conventional lines with shared traffic (freight and passengers).

3.2.1.2 Mainline Passenger Railways

It is assumed that for the VCTS functionality to be available for Mainline Passenger Railways

- the wayside installation of the enabling area is a system that follows the ERTMS architecture and includes an RBC and
- the trainborne installation on the involved trains also follows the ERTMS architecture and includes an ATO.

The actors of the Mainline Passenger Railways use-case are the following (see Figure 14):

- Strategic Layer
  - Requests missions from the VCTS
  - Receives feedback with denial or permission of a mission
- ATO
  - Derives the Operational Dynamic Speed Profile from the VCTS
- OBU

- Derives the Vital Dynamic Speed Profile from the VCTS
- Train Driver
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- ATS
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- RBC
  - Derives the VCTS Status
- Neighbour VCTS
  - Establishes the Link
  - Provides Control Data
  - Receives Status Data

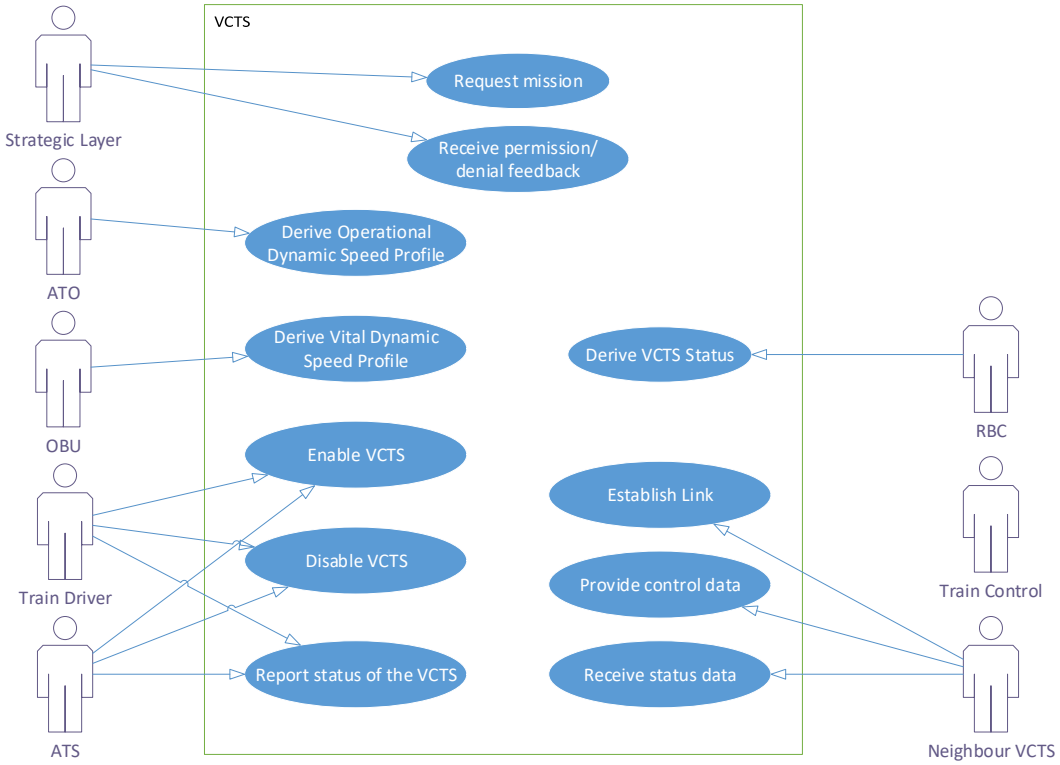

Figure 14: Use Case Diagram for Mainline Passenger Railways

The potential performance gains provided by VCTS for Mainline Passenger Railways are:

- Reducing headway further; approaching relative braking distance (convoys) to increase the capacity of existing lines that cannot be easily improved through civil works (e.g., commuter lines in city centers running through tunnels).
- Increasing performance at bottlenecks between junctions (especially for layouts without stations between the junctions)

3.2.2 Local/Low Density Railways

Local/Low Density railways, with their unique operational characteristics and constraints, require a tailored approach to signalling and control systems. The focus is on optimizing the layout of system components to meet specific capacity requirements while ensuring safety and efficiency.

It is assumed that for the VCTS functionality to be available in a Local/Low Density Railway area

- the wayside installation of the enabling area is a legacy system that does not follow the ERTMS architecture
- the trainborne installation on the involved trains also does not follows the ERTMS architecture
- a VCTS standalone solution is deployed

The actors of the Local Railways use-case are the following:

- OBU
  - Derives the Vital Dynamic Speed Profile from the VCTS
- Train Driver
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- ATS
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- Train Control
  - Receives Control Commands
- Neighbour VCTS
  - Establishes the Link
  - Provides Control Data
  - Receives Status Data

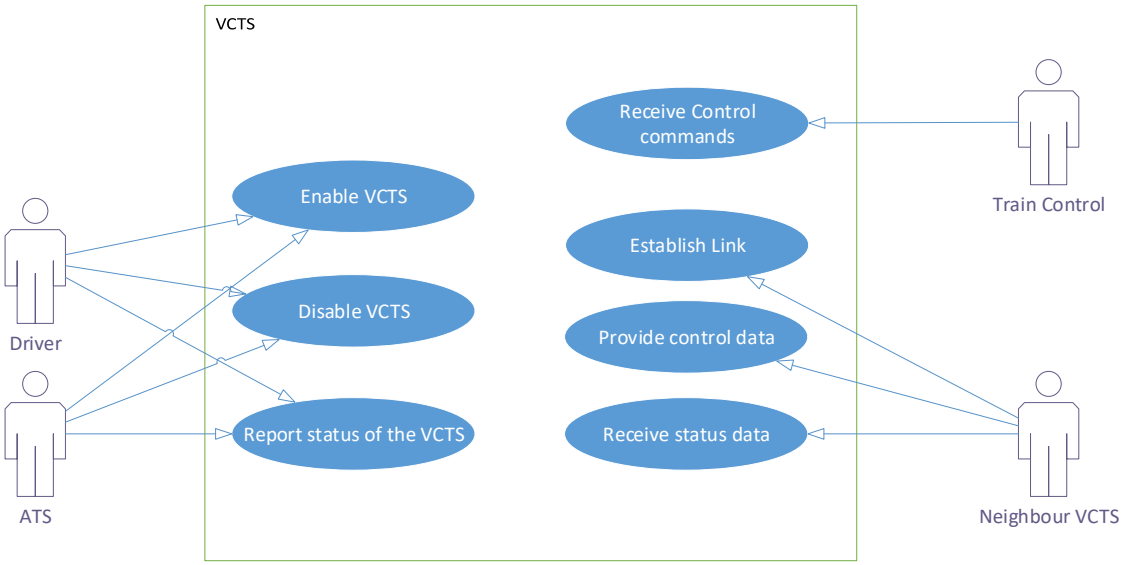

Figure 15: Use Case Diagram for Local/Low Density Railways

The potential performance gains provided by VCTS for Local/Low Density Railways are:

- Increasing throughput on rudimentary equipped lines
- Increasing performance on single track lines
- Adding an additional safety layer (T2T communication, informing about location of the next train, etc.), see also section 3.3.3

3.2.3 Mass Transit/Urban Railways

Mass Transit and urban railways are at the forefront of adopting sophisticated signaling systems to meet the demands of high-density passenger flow and operational efficiency. The focus is on centralized monitoring systems to ensure smooth operation and reduce monitoring delays. The design and development of data communication subsystems within Communication-Based Train Control (CBTC) systems are critical for maintaining safety and reliability in urban rail transit.

It is assumed that for the VCTS functionality to be available in a Mass Transit/Urban Railway network the wayside and onboard installations constitute a CBTC system at least allowing for Grade of Automation 2 (GoA2) operations.

The actors of the Mass Transit use-case are the following:

- ATO
  - Derives the Operational Dynamic Speed Profile from the VCTS
- VOBC
  - Provides the ATC Status to VCTS
  - Provides Vital Location information to the VCTS
  - Derives the Vital Dynamic Speed Profile from the VCTS
- Train Driver
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- ATS
  - Enables the VCTS
  - Disables the VCTS
  - Receives indications on the VCTS status
- ZC
  - Derives the VCTS Status
- Neighbour VCTS
  - Establishes the Link
  - Provides Control Data
  - Receives Status Data

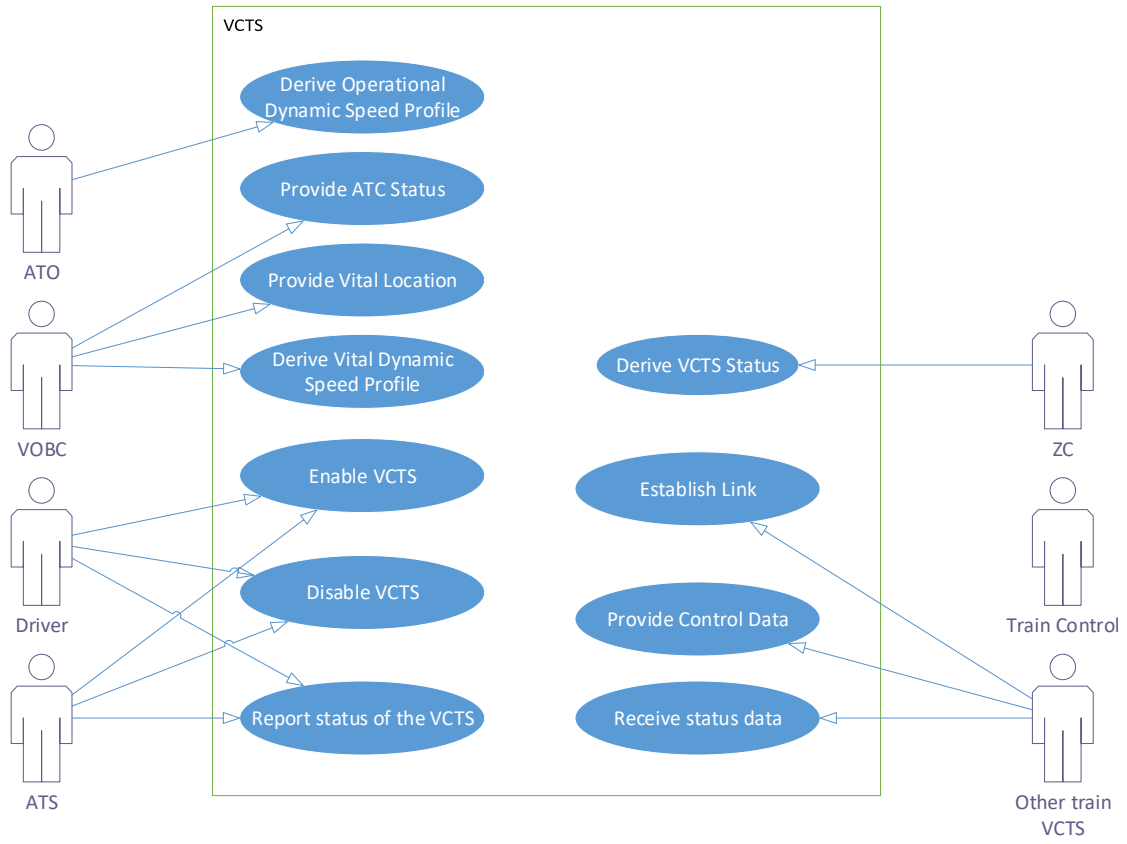

Figure 16: Use Case Diagram for Mass Transit/Urban Railways

Potential performance gains:

- Reducing headway towards relative braking distance (convoys)
- Increasing capacity of train services “on-the-fly” without the need for actual coupling
- Increasing performance at bottlenecks between junctions (especially for layouts without stations between the junction

3.2.4 Summary of Use-Cases

Potential use-cases for VCTS functionality exist across various railway systems, but they show differences in relation to their specific operational contexts, potential performance gains, and the roles of different actors involved.

Each use-case aims to reduce headway, increase capacity, and improve performance at bottlenecks.

To implement VCTS (Virtual Coupling Train System) effectively, several considerations must be taken into account based on the use-cases described in the document:

3.2.5 System Architecture

• Mainline Passenger and Freight Railways: These systems strive to follow the ERTMS architecture, which includes RBC (Radio Block Center) and ATO (Automatic Train Operation) installations. This ensures compatibility with existing signaling systems and facilitates the integration of VCTS.

- Local/Low Density Railways: These railways utilize a legacy system that does not follow the ERTMS architecture. Therefore, a standalone VCTS solution is required to ensure proper functionality.
- Mass Transit/Urban Railways: As state of the art these systems implement a CBTC (Communication-Based Train Control) system that allows for GoA2 to GoA4 operations. This advanced signaling system supports the high-density passenger flow and operational efficiency required for urban rail transit.

3.2.6 Operational Focus

- Mainline Passenger Railways: The focus is on increasing the capacity of existing lines, especially in city centers where civil works are challenging. VCTS can help reduce headway and eventually approach relative braking distances, thereby enhancing line capacity.
- Mainline Freight Railways: The emphasis is on reducing headway to absolute braking distance and improving performance on shared traffic lines. This is crucial for optimizing freight operations and increasing throughput, e.g. at bottlenecks between junctions, especially for layouts without stations between the junctions.
- Local/Low Density Railways: The goal is to optimize throughput on rudimentary equipped lines and single-track lines. VCTS can add an additional safety layer through train-to-train communication, informing about the location of the next train.
- Mass Transit/Urban Railways: The priority is on centralized monitoring and data communication subsystems to manage high-density passenger flow. VCTS could allow to increase the capacity of train services "on-the-fly" without the need for actual coupling by reducing the headway to relative braking distance**.**

3.2.7 Key Considerations

1. Compatibility with Existing Systems: Ensure that VCTS is compatible with the existing signaling and control systems, whether it is ERTMS, legacy systems, or CBTC.
2. Operational Efficiency: Focus on the specific operational needs of each railway type, whether it is increasing capacity, reducing headway, or optimizing throughput.
3. Safety Enhancements: Implement additional safety layers, such as train-to-train communication, to enhance overall safety.
4. Performance Optimization: Aim to achieve the potential performance gains identified for each use-case, such as increasing capacity and improving performance at bottlenecks.

By addressing these considerations, the implementation of VCTS can be tailored to meet the specific needs and challenges of different railway systems, ensuring enhanced operational efficiency and

3.3 DEFINITION OF OPERATIONAL CONCEPT AND BASELINE

According to the standard ISO/EEC/IEE 29148:2018 an operational concept description is used to communicate overall quantitative and qualitative system characteristics to the acquirer, user, supplier and other organizational elements [23]. It describes what the system will do and why. The operational concepts allow engineers to find ways to address the mission and objectives of systems under development. It will set high level requirements and objectives pointing to critical aspects of the operation. The VCTS operational concept is described in detail in the X2Rail3 [24]. The most important aspects of the concept along with its two baseline applications identified in [25], ETCS L2 Moving Block and VCTS Standalone Application will be outlined in this subchapter.

3.3.1 Outline of General VCTS Concept

Today's railway operations often rely on either fixed block or moving block policies for train MA. In the moving block approach, the trains are able to determine their own rear end position and update the signalling system to set the MA of train to the rear of MA directly at the end of the next train. This strategy reduces the required minimum headway compared to the fixed block approach. However, despite its advantages, there are opportunities for further improvement and optimization in the implementation of the moving block approach.

In the current Moving Block System, block size calculation is based on ABD determined by real-time velocity. This means that the block size is defined to ensure the following train can safely come to a full halt, even if the preceding train stops instantaneously. However, in reality, the preceding train's braking is not instantaneous due to inertia, and its braking distance varies depending on speed and braking characteristics. Consequently, the ABD-based block size tends to be higher than what is actually necessary with the existing train protection functions (D6.1) and ETCS L2 moving block communication capabilities. With accurate real-time information on train statuses and braking capabilities available to the RBC, the need for ABD is reduced, making way for the concept of VCTS.

VCTS is a concept that will shift the braking paradigm from the current ABD to relative brake distance (RBD) as shown in Figure 17. This transition will allow trains to operate at much closer distances, consequently increasing track capacity. This also brings new possibilities to the traditional train coupling methods. Traditionally, trains are coupled mechanically depending on their destination, compatibility and schedules. The mechanical couplers were used to maintain relative distance, for force transmission and information exchange. In VCTS the mechanical links will be replaced by virtual links using continuous, safe and reliable wireless communication technology. Without the mechanical link, the leading trains cannot transmit the forces and maintain distance. Therefore, the trains need to be able to move independently in a platoon and regulate their own relative distances with other trains.

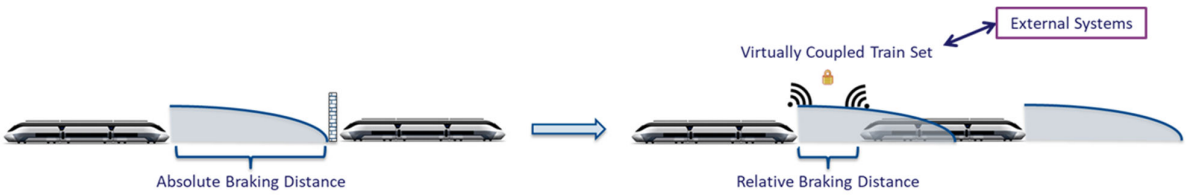

Figure 17: Absolute Braking Distance vs Relative Braking Distance **[24]**

The VCTS will have a set of functions to group trains as a platoon which can safely form a platoon, drive as one unit and decouple during transit. Therefore, core functionality of VCTS is to safely maintain a controlled and coordinated headway between the trains in the platoon and to keep the headway minimum. In order to achieve this, each train in the platoon needs to be able to compute

its own headway. The VCTS system decides the cooperative driving strategy and provides each train awareness of its own characteristics and environment to compute and supervise their own headway. To achieve this, each train in the platoon requires the following information:

- Its own specific braking characteristics.
- The characteristics of other trains in the platoon.
- Real time dynamics information of other trains in the platoon.
- Information about track conditions

The performance of VCTS depends upon the technological choices made for its various components. Several potential benefits of VCTS were identified in [24] , which are listed below:

- Increase **line capacity** by reducing the headway
- Enhance **line efficiency and operational flexibility** by reduced coupling time and new consist building procedures
- Platoons can be established or dissolved while in operation
- Faster platoon building procedures
- Increased **robustness of schedule**
- Gaining **interoperability** between different vehicle models, types or manufacturers
- Enabling vehicles to **operate in different signaling systems**
- Maximized **utilization of platforms** and **passenger comfort**
- Reduce global **investment-, maintenance- and operational costs**
    - Adding on-board and trackside signaling/electronic systems, instead of tracks or heavy changes of the infrastructure
    - Reduction of materials (cables, etc.) and therefore mitigation of weight- and design constraints of rolling stock
    - Omission of manual coupling procedures or sidetracks
- Increase **competitiveness** in railway freight and passenger transportation against road transportation.

3.3.2 VCTS Application ETCS L2 / ETCS L2 Moving Block (High-Traffic Lines)

The objective of ETCS L2 and ETCS L2 Moving Block systems are to improve capacity, lower cost, improve reliability of signalling system across all railway market segments. With ETCS L2, capacity and reliability are improved through more accurate reporting of train positions to the RBC and smaller block sizes compared to legacy signalling systems. Lower cost is achieved through fewer lineside signals, which in turn reducing the probability of signal failures, disruptions and maintenance costs.

With ETCS L2 Moving Block, this goes a step further. Higher capacity is achieved through the use of moving block principles, which enable trains to determine their own minimum safe rear-end, relying on onboard train integrity functions. This way, the RBC can extend Movement Authorities (MA) for a train arbitrarily up to the rear of the train in front. Lower cost is achieved by reducing the use of trackside train detection and line-side signals since the RBC receives necessary information related to track occupancy from the trains directly. High reliability is achieved as a consequence of the reduction in trackside equipment associated with trackside train detection and line-side signals.

In practice, Level 2 Moving Block has evolved into an intermediate concept known as Hybrid Level 2, explored in WP15 and 16, which combines elements of Level 2 with the introduction of Hybrid Train Detection (HTD). This hybrid approach allows for a progressive transition from fixed blocks to mobile blocks, ensuring greater compatibility with existing infrastructure and facilitating the implementation of cutting-edge technologies in railway operation

The primary objective of integrating the Virtual Coupling Train System (VCTS) within the framework of ETCS L2 and ETCS L2 Moving Block is to enhance the line capacity, operational efficiency and flexibility of high-traffic railway lines even further. VCTS aims to overcome specific challenges, particularly focusing on moving towards more train centric signalling approach and changing the braking distance paradigm from ABD to RBD. By doing so, VCTS aims to reduce the safe distance maintained in ETCS L2 and ETCS L2 moving block system, thereby increasing the line capacity. Furthermore, it will reduce time required coupling trains in comparison to the conventional methods which further improves capacity and flexibility.

VCTS can be introduced in two stages to accommodate varying levels of railway infrastructure development. The first stage of VCTS will replace the function of the mechanical coupler. Coupling and decoupling operations will be carried out at stations while trains are stationary. Once coupled at a station, the trains will operate as a single unit to a common destination and then separate at a subsequent station to follow their individual routes. This approach will reduce the time required for coupling and decoupling, thereby increasing system robustness. Additionally, it will enable the coupling of trains that were previously incompatible due to differing coupling mechanisms, enhancing interoperability and operational flexibility. This stage of implementation will also allow multiple trains to stop safely in close proximity at stations, one behind the other, improving platform utilization and overall operational efficiency. The changes required in this stage will primarily be onboard, including integration of VCTS-OB systems with ATP and ATO systems, with minimal modifications needed to existing trackside ETCS systems for movement authority allocation and interlocking.

The second stage of VCTS will use advanced communication and control systems to manage virtual platoons dynamically. Unlike physically coupled trains or first stage of implementation, this stage enables dynamic adjustment to the composition of virtual platoon based on operational requirements. Trains can join or leave a platoon as needed while in motion, providing flexibility in adapting to changing conditions such as variations in passenger demand, speed profiles, or operational constraints. This allows more flexibility and optimized exploitation of available track capacity, further increasing operational efficiency and flexibility. The VCTS concept can rely on ETCS L2 Moving Block technologies with additional T2T communication for operation as shown in Figure 18.

Implementing VCTS in the second stage will require several key technical enablers to integrate with the existing ETCS Level 2 Moving Block infrastructure. These include modifications to both on-board and trackside subsystems. At the interface level, VCTS requires interaction with the ETCS on-board unit, particularly for platoon status and activation functions. Additionally, the TMS must be equipped with an interface to the VCTS on-board equipment to support mission monitoring.

Functionally, changes to the Radio Block Centre (RBC) are essential to incorporate the concept of virtually coupled platoons. The RBC and TMS must be capable of perceiving and managing the dynamic length of platoons and the changing number of units involved between stations. On-board, additional VCTS equipment will interface with ATP and ATO systems to support coordinated operation. Furthermore, new communication protocols for train-to-train (T2T) and train-to-ground (T2G) communication will be required to ensure seamless and reliable data exchange between trains and the infrastructure.

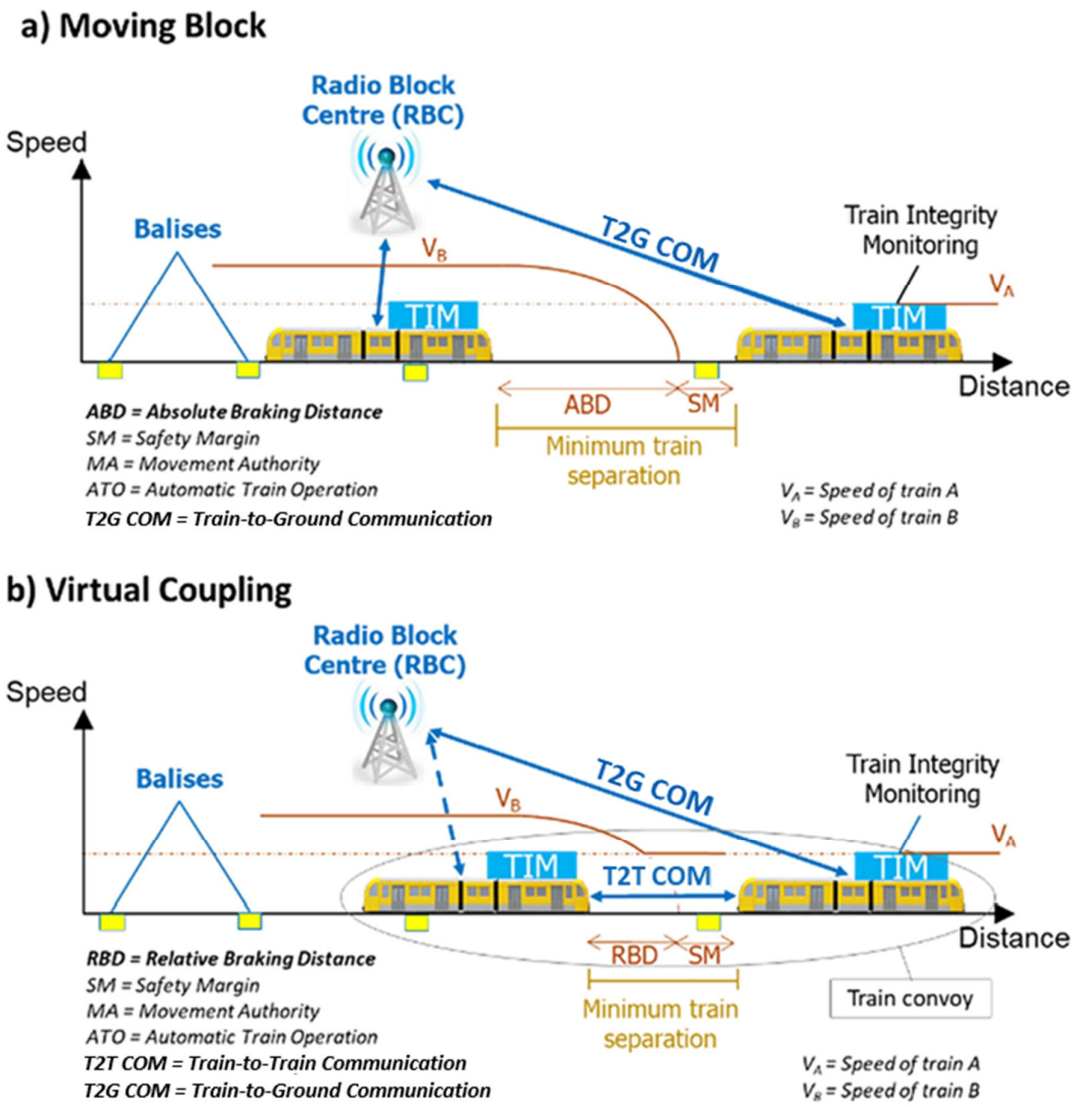

Figure 18: Moving Block architecture and Virtual Coupling architecture adapted from **[26]**

3.3.2.1 Operational States and transitions

In [26] VCTS was modelled and simulated, and 5 different operational states where identified which are illustrated in the flow diagram in Figure 19.

State 1 ERTMS: This state refers to scenarios when both trains A and B are running independently at speeds V_A and V_B respective and operating under ERTMS signalling principles. During this state depending on the signalling system in place, a minimum distance of absolute braking distance with safety margin is maintained with the preceding trains and no train to train communication is established. The safety margin (SM) is always taken into account during manoeuvres to ensure collision is avoided in case of positioning errors or gap overshoots due to controller error.

State 2 Coupling: If trains A and B are sharing a common route, they can be coupled to allow more movement authority for other trains. In such a scenario the trains enter into the coupling state. During the coupling state the trains will initiate communication and exchange relevant data with each other to coordinate speeds in order to gradually reduce the gap between them from ABD plus SM to RBD

plus SM. In the first stage of implementation this will be done at the station, where train A will be stationary and train B will approach train A at very low speeds to reduce the gap between them to enter coupled state. In second stage of implementation the gap can be reduced by either train B increasing its speed from V_B to V'_B or train A reducing its speed from V_A to V'_A.

State 3 Coupled running: When the trains have coordinated their speeds and attained the safe gap according to virtual coupling principle, the coupled running mode is initiated. In the coupled running mode RBD plus SM is maintained between all trains in the platoon by communicating dynamic state information between the trains in the platoon. In this state the whole convoy of trains that are coupled should be treated as a single unit by the signalling systems and the speeds will be dictated by the leader of the platoon in this case train A.

State 4 Unintentional Decoupling: Unintentional decoupling state refers to scenarios where the following train B is unable to maintain the minimum safe distance with train A due to different traction limitations or gradients. In such scenarios the train B will transition back to coupling state and couple again when the conditions allow it. In first stage of implementation if this exceeds the allowed threshold safe distance allowed it should be treated like integrity loss.

State 5 Intentional Decoupling: Intentional decoupling is state in which trains in the platoon need to leave the platoon because they no longer have a common mission. For the first stage of implementation this will be done at a station. Both trains will come to halt and the train-to-train communication is terminated and each unit reverts back to State 1. For the second stage of implementation the gap between the trains is increases to a minimum of ABD plus SM by either reducing speed of the following train B or increasing the speed of the lead train A depending on the mission constraints. Once distance more than ABD plus SM is achieved the trains terminate the communication with each other and take over the control and execute their independent missions following ERTMS principles.

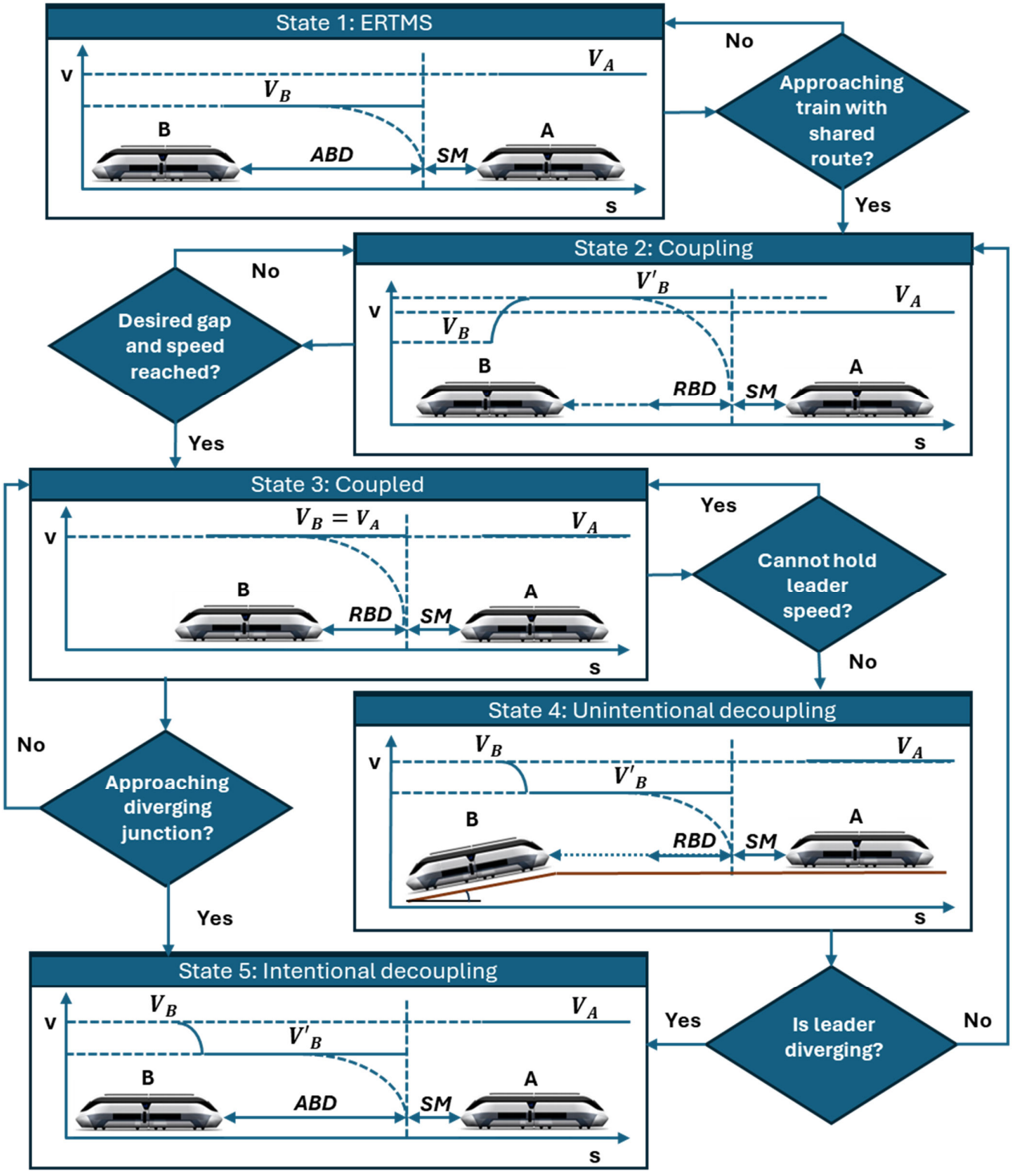

Figure 19: VCTS Operational States

3.3.3 VCTS Standalone (Low-Traffic Lines)

This application baseline refers to non-SERA low-traffic regional lines with basic or legacy signalling systems facing obsolescence which were identified in [25]. These lines, are often not prioritized for ETCS deployment due to high costs relative to low traffic density, typically involve small multiple units and may lack electrification. The current basic ATP functionalities on these lines are often minimal, relying on station dispatchers in scenarios where TMS is absent, and speed supervision is lacking.

The introduction of a new reference architecture, moving block, and ATO regulations poses challenges for Infrastructure Managers (IM) and Railway Undertakings (RU), with thousands of kilometres yet to migrate to ETCS. The incorporation of disruptive technologies like VCTS into ERTMS is considered risky at this stage, potentially compromising stability. However, there is an opportunity to implement VCTS with lower complexity on non-ETCS lines with low traffic density as a cost-effective solution. It can address obsolescence challenges by replacing legacy signalling systems and introducing a new vehicle-centric protective layer to replicate and/or complement ATP safety functions already in place, especially where ETCS implementation is economically unfeasible.

The objective of VCTS in this application is not to increase line capacity but to serve as an onboard system that can be used for mutual supervision of other trains on the track, for train protection when necessary and for continuous speed supervision at a low cost. Therefore, the VCTS standalone system will be designed to operate with lower complexity and reduced performance compared to high-traffic applications. This means that the focus is not on achieving higher capacities by driving with headways less than ABD, but rather on enabling trains to be aware of their environment and other trains on the track, and to safely compute and manage headway onboard. This will be achieved through communication-based mutual supervision, relying on two key technologies: absolute and safe train positioning without infrastructural inputs and safe communication through public networks.

On the low traffic lines, normally trains run at distances much larger than ABD between them. Therefore, the VCTS does not need to maintain short distances or form platoons like in ETCS L2 and L2 moving block application. However, if it is required that the trains need to be at distances closer than ABD the VCTS system should act as protection layer. The system will behave like a moving block system but with reduced performance. The last known rear end position of the other train on the line will be used as reference for MA.

The VCTS standalone system will retain the general architecture. The main difference, in contrast to the high-traffic line application of VCTS, is that the information exchange required for safe cooperative movement, headway management in this case may be conducted over public networks, such as existing 4G or 5G infrastructure network. This makes the system applicable to all railway lines, since it can leverage existing infrastructure, reducing the initial investment required to deploy VCTS while improving efficiency of such lines.

An exemplary functional architecture for this application is shown in Figure 20. In this configuration, the TMS represents the strategic layer of VCTS and maintains a network-wide view of train positions, speeds, integrity, status, and timetable information. Based on this information, the TMS is responsible for allocating missions, initiating information exchange between trains, and assigning roles to involved trains to execute the missions.

Each train is equipped with a VC-OBU that receives information of its own absolute position, integrity from the onboard ASTP unit, and Onboard Train Integrity system, respectively. The trains are also equipped with T2T communication systems. The VC-OBU receives information from the TMS

including role assignment, type of maneuvers, and train IDs relevant for the mission. The mission execution and the cooperative movement are coordinated by the respective VC-OBUs through exchange of relevant information via the public 4G/5G network while continuously updating the TMS on the status.

Under normal operating conditions on low-traffic lines, the trains operate with relatively large spacing. In this baseline mode, VCTS provides mutual awareness by exchanging absolute position, speed, and train integrity information via the public network. Safe operation can therefore be achieved with relatively low update rates, and direct T2T functionality remains supervisory. This mode of operation is illustrated by the interactions between Train B and Train C in Figure 20.

When two trains begin to operate at decreasing separation or when predefined safety thresholds are approached, the onboard T2T module takes an ATP-like protection role. In this case, the T2T module initiates direct communication between relevant trains. This direct exchange of relative position, velocity, and train integrity at higher and more reliable update rates allows the VC-OBU to locally supervise the separation and, if needed, trigger protective actions to prevent unsafe approach, independent of the public communication networks and without reliance on trackside ATP infrastructure. This mode of operation is illustrated by the interactions between Train A and Train B in Figure 20.

On rural lines where shorter headways are necessary or beneficial, the same configuration could also be used to transition to full coupling. The TMS may initiate full coupling, and the VCTS-OBU can support closer proximity operation. However, in the absence of continuous and reliable long-range T2T communication, full coupling will be limited to scenarios where at least one train is stationary, typically at stations, where the coupling train can slowly approach the stationary train to fully couple and depart the station as a coupled train set.

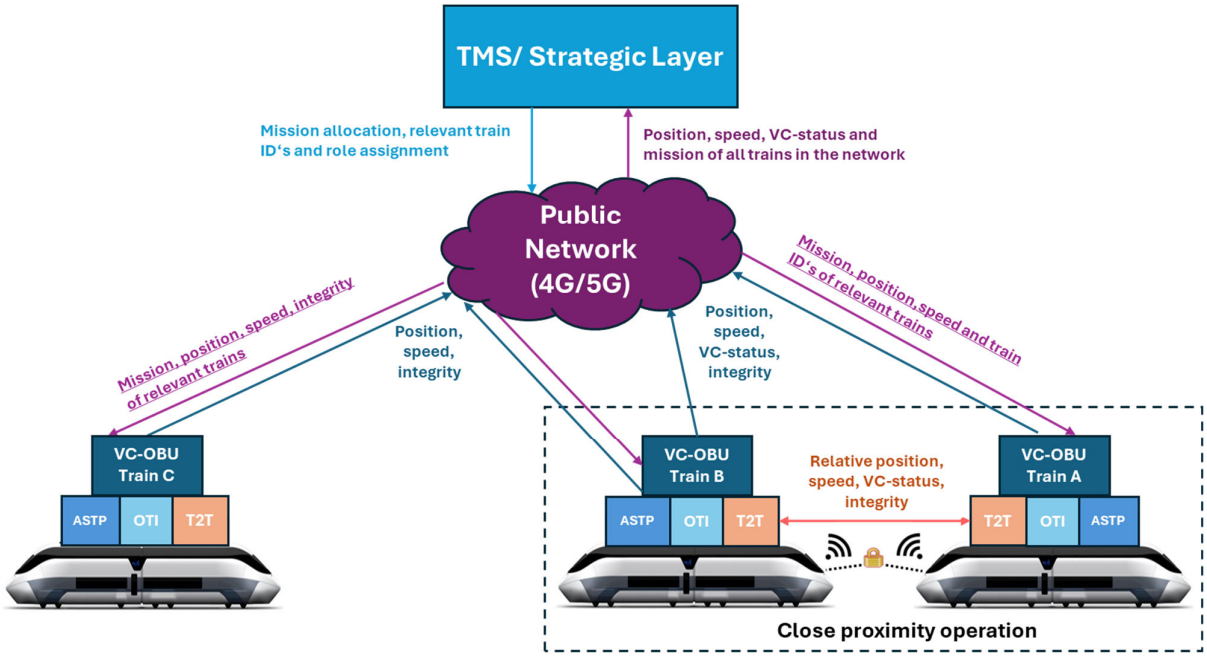

Figure 20: Exemplary Functional Architecture for VCTS Standalone

In VTCS standalone application the trains will be driving independently. The VCTS system is only used as a safety layer that connects the trains for mutual supervision and intervenes only when necessary. The train drivers will follow the signals and speed limits remaining on the tracks and will use the speed limits provided by the VCTS if the distance to the train in front is getting closer.

This approach combines several advantages of a train centric signalling system which were identified in [25]:

- Existing interlocking could be reused, or optionally upgraded for improved performance
- Almost no infrastructure elements required (e.g. no balises)
- No complex TMS required
- Provides increased safety
- Utilization of public communication systems (4G or ideally 5G), no specific railway system (GSM-R / FRMCS) required
- Possibility to easily transition to higher ETCS levels if needed.

For the integration of a VCTS standalone application on low-traffic lines, several key points need consideration. Achieving safe and reliable communication through a public network and implementing new communication protocols for trains to communicate with each other over the network are necessary for implementing this system. Furthermore, cybersecurity for communication through public networks also needs addressing. Existing infrastructure elements can complement VCTS mutual supervision. Most modifications will occur onboard. New absolute location systems, a 4G/5G router, and old onboard ATP components and software should be replaced with VCTS standalone systems with interfaces to the driver.

To summarize, the VCTS standalone application will behave like a moving block system with lower performance and complexity. It aims to challenge the obsolescence issue of the existing signalling on low traffic lines where ETCS implementation is not economically feasible. It can be deployed on any kind of line as a cost-effective ATP system since no infrastructure elements are required. It offers a cost-effective and flexible solution that aligns with evolving industry landscapes and regulatory requirements. The solution also ensures a smooth transition towards higher ETCS levels if required.

3.4 DEFINITION OF TECHNOLOGICAL BASELINE

VCTS enables train consists within a platoon to move at distances below their respective absolute braking distances. It further allows them to dynamically compose/decompose platoons on the move. These capabilities are dependent on different subsystems of the railway system, the main ones identified for the VCTS system design are CCS, Communications, Localisation, and Train Integrity Monitoring (TIM). In the following, the technological baseline for these subsystems for the EU Rail VCTS concept is presented.

3.4.1 Control Command and Signalling (CCS)

The CCS subsystem is defined in Annex II to Directive (EU) 2016/797 as *“all the trackside and on-board equipment required to ensure safety and to command-and-control movements of trains authorised to travel on the network”.* The safety, reliability and availability objectives of the CCS are apportioned between the trackside and on-board components, each serving distinct yet interdependent roles.

ERTMS is one of the key initiatives aimed at standardising CCS across Europe. In 2000, UNISIG, an organization of European signalling companies, developed the initial ERTMS technical specifications. The European Commission integrated these specifications into the technical requirements for interoperability (TSI) for the trans-European high-speed rail system with Commission Decision 2002/731/EC and for the conventional rail system with Commission Decision 2006/679/EC. The technical specifications for both high-speed and conventional railways were later unified under Commission Decision 2012/88/EU.

The first stable set of ERTMS specifications, considered interoperable at the European level, includes the ETCS with baseline[1] 2 for automatic train protection (ATP) and GSM-R with baseline 1 for radio communication. Subsequently, in 2016, ERTMS specifications with ETCS baseline 3 release 2 were issued while also incorporating GPRS into the GSM-R specification. This release represents a mature and stable version of ERTMS, able to solve any interoperability issues.

The most recent ERTMS specifications adopted by the European Commission under Regulation (EU) 2023/1695 include ETCS baseline 4 release 1 (B4 R1), ATO with baseline 1 release 1 (B1 R1), and a Railway Mobile Radio (RMR) system with GSM-R baseline 1 maintenance release 1 (B1 MR1) and FRMCS baseline 0 (B0). RMR may be implemented with both GSM-R and FRMCS together or each of them independently (FRMCS with certain requirements on finalized specifications and maturity). Figure 21 shows an overview of the ETCS B4 R1 reference architecture [27] with trackside and on-board components along with their interfaces. The following discussion on the CCS technological baseline for VCTS uses ETCS B4 R1 as a starting point.

Different ERTMS/ETCS application levels are defined depending on how the trackside is equipped, how the information is transmitted to the train, and which functions are processed in the trackside and on-board components [27]:

- Level 0 (L0): train equipped with ETCS operating on a line not equipped with any train control system (ETCS or national system) or on a line equipped with ETCS and/or national system(s) but operation under their supervision is currently not possible.
- Level NTC: train equipped with ETCS operating on a line equipped with a national system.
- Level 1 (L1): train equipped with ETCS operating on a line equipped with Eurobalises (and Euroloop or Radio infill on existing lines but not new ones except in special cases). Eurobalises are ground-based transponders explained in subsection 3.4.2.1.
- Level 2 (L2): train equipped with ETCS operating on a line controlled by a Radio Block Centre (RBC) and equipped with Eurobalises and EURORADIO communication over RMR. Train detection and train separation are performed by the RBC based on position reports and train integrity information received from the train and/or by other trackside equipment outside the scope of ETCS.

ETCS L1 and L2 have traditionally been characterized by fixed block sections and trackside signals ensuring safe train operations. In this system, train movements are authorized up to the front end of the section adjacent to an occupied one. When a train enters a track section, the entirety of that section becomes unavailable for other trains. Although this approach with predefined sections has

[1] The baseline is a stable kernel in terms of system functionality, performance, and other non-functional characteristics. It is not to be confused with ETCS *level*, which is explained further below.

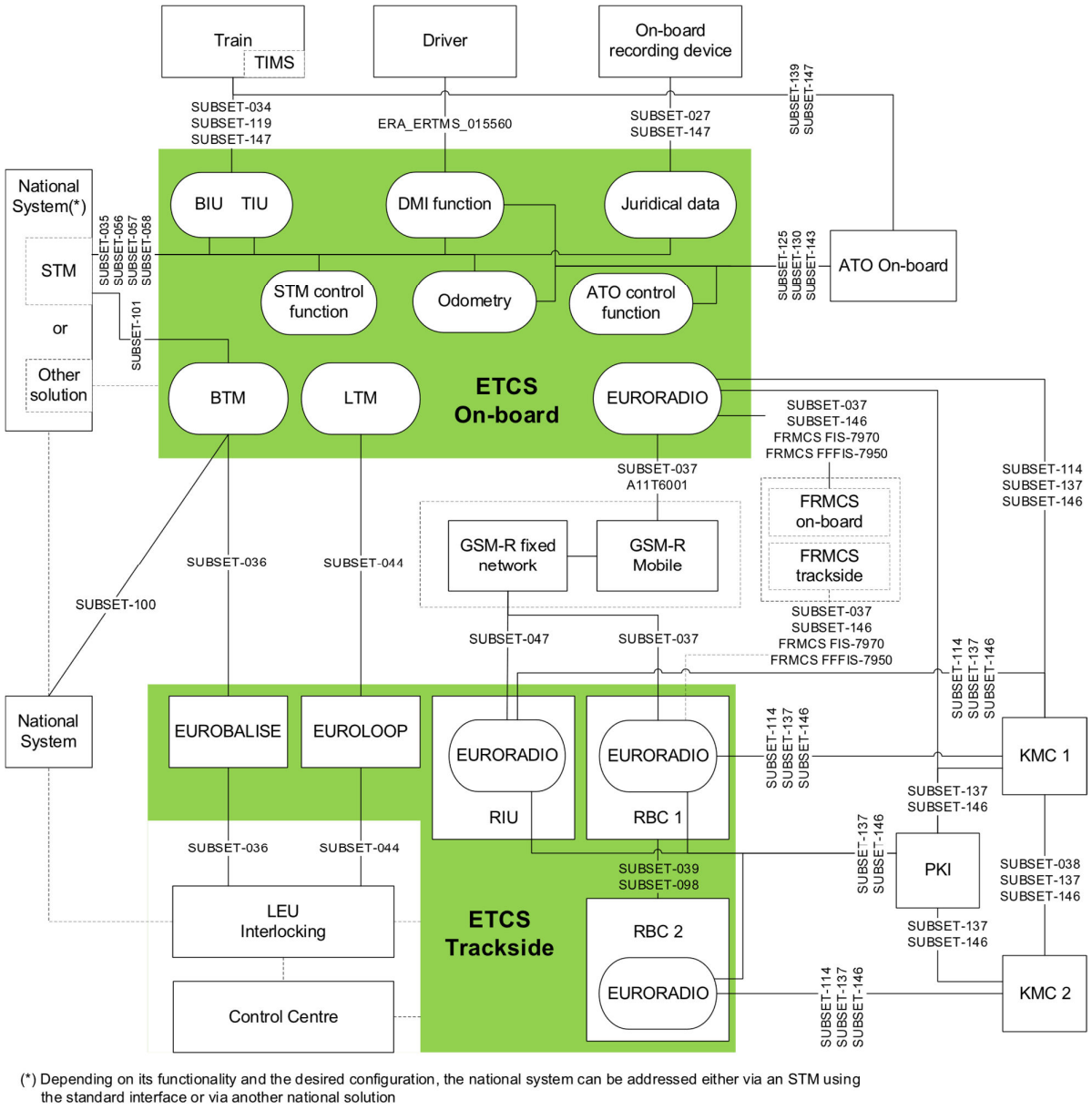

Figure 21: ERTMS/ETCS baseline 4 release 1 reference architecture **[27]**

proven to be effective in enhancing safety, it imposes constraints on the attainable operational capacity and flexibility with existing tracks.

To overcome these limitations, the L2 in the latest ETCS B4 R1 now includes support for a moving block approach (formerly ETCS Level 3 (L3) [28] [29]) where the end of a track segment is made optional. With this modification, train movements can be authorized up to the rear end of the preceding train, incorporating an additional safety margin. The RBC generates these movement authorities for individual trains by safely determining the rear end of the trains using position reports and train integrity information from the trains. In this “moving block” approach, tracks do not need to be divided into predefined sections, thereby increasing operational flexibility. Nonetheless, the capacity improvements are limited since the trains must be able to fully stop at the last known position

of the rear-end of the train ahead irrespective of the current speed and braking curve of the train ahead.

Although ETCS B4 R1 may technically allow certain VCTS functions to be integrated within its current framework, this is limited to the first stage of VCTS as described earlier in subsection 3.3.2, i.e., replacing mechanical coupling with virtual coupling while trains are stationary in stations. In this case, coupling and decoupling operations occur only at standstill, and the virtual platoon composition remains fixed during motion. To fully benefit from VCTS, including dynamic adjustment of the virtual platoon composition while trains are in motion, additional modifications are required, not only to the on-board but also to the trackside subsystems, particularly in how they perceive, manage, and authorize movements for dynamically varying platoon lengths. Such functionality goes beyond what ETCS B4 R1 currently supports and requires a more modular and evolution-ready system architecture.

Moreover, today's railway architecture is the result of many decades of small component-wise transformations and is considered inflexible, difficult to integrate, and expensive to migrate and replace. The persistence of legacy CCS systems is a significant barrier to an optimized and unified railway system [30]. Until recently, the absence of a unified EU-level vision for the future railway system architecture allowed national and regional networks to continue developing along divergent technical trajectories. In response to this long-standing fragmentation, the Europe's Rail Joint Undertaking established the System Pillar (SP) consortium to ensure that the evolution of the rail system is based on common operational visions and a formal functional system architecture approach. However, at the time of this drafting in November 2023, which served as groundwork for the subsequent chapters, there were no architectural outputs available from the SP. Given these limitations of both ETCS B4 R1 for advanced VCTS integration and the constraints of today's legacy-driven CCS landscape, we therefore examined more recent publicly available and technically developed—yet still evolving—architectures that offer a more flexible and sustainable pathway for integrating VCTS. Furthermore, based on discussions with experts, the SP architecture of the on-board CCS subsystem is expected to be aligned with the Open CCS On-board Reference Architecture (OCORA), presented in subsection 3.4.1.1. While no specific indication has been received from SP regarding the trackside CCS subsystem, the Reference CCS Architecture (RCA), presented in subsection 3.4.1.2, from the EULYNX initiative is closely related to OCORA and can be expected to have a fundamental impact on the discussions within SP. Thus, the most recent releases of OCORA (Release 4) and RCA (Baseline 1 Release 0) available at the time of this drafting are considered as the technical baseline for CCS within the scope of this document.

It is worth noting that, following the drafting of this chapter, SP has made notable progress, including the public releases of a Traffic Control and Supervision (CS) System concept [1] and a Train CS architectural baseline [2]. A detailed analysis of the differences between the selected OCORA and RCA architectural baseline and the emerging System Pillar's CS architecture is necessary to ensure that VCTS technological developments are consistent with the ongoing System Pillar's work. However, such a comparison is beyond the scope of this document and will be addressed in future work.

3.4.1.1 Open CCS On-board Reference Architecture (OCORA)

The OCORA cooperation platform [30] was established by five railway undertakings (RUs): Deutsche Bahn AG (DB), Schweizerische Bundesbahnen AG (SBB), NS Groep N.V. (NS), Société nationale des chemins de fer français (SNCF), and ÖBB-Produktion GmbH. The initiative envisions a coherent, modular, upgradeable, interchangeable, reliable, and secure system architecture to overcome the

challenges of the current CCS on-board (CCS-OB) solutions. It acknowledges the urgency of taking immediate and decisive measures to deal with the technological innovations in railways, as well as a smooth transition of the legacy systems such as the existing ERTMS infrastructures and the onboard ETCS installations. Considering both short- and long-term perspectives, OCORA adopts a progressive and incremental architectural framework.

In the short term, OCORA intents to contribute to an unambiguous standardization of the interface between the CCS-OB and the Vehicle Environment which includes the TCMS, and other operator subsystems. The OCORA proposes a Train Adapter (TA) to abstract the specificities of each train and aims to achieve consistency in the CCS-OB system for both legacy and new-generation vehicles. The CCS-OB system is modularized into several independently procurable building blocks[2] that can be exchanged/upgraded without affecting other building blocks, simplifying the life-cycle management. In the long-term OCORA vision, the CCS-OB system contains a safe computing platform which hosts the core CCS functions as applications (software building blocks) and TA will no longer be needed.

The documents from OCORA release R4 considered here contain CCS-OB logical and physical architecture, as well as technical and program documentation of various topics. The CCS-OB system is designed to support ETCS L0 to L2 moving block, level NTC, ATO GoA 1 to 4 over ETCS, GSM-R and/or FRMCS connectivity, and the potential to implement Notified National Technical Rules (NNTRs). Figure 22 and Figure 23 show the logical architecture of the CCS-OB system for legacy trains highlighting internal and external block exchanges. Figure 24 shows the physical architecture of the CCS-OB system with hardware and software building blocks for the legacy train. For new-generation trains, the logical and physical architectures are very similar to the legacy train, except that the TA is no longer required. The block exchanges are realized by one or more standardized interfaces (see Table 3 in [31]). The identified external actors interacting with CCS-OB are grouped into:

- **Operation Control Systems – Infrastructure Manager (OCS-IM):** contains CCS trackside (CCS-TS) components such as the Incident and Prevention Management – Incident Solving Manager (IPM-ISM), RBC & Movement Authority Transactor (MT), ATO Transactor (AT), Traffic Management System (TMS), Key Management Centre (KMC), and Voice Communication System (VCS) etc. Some of these trackside components are of primary focus in RCA and are further described in subsection 3.4.1.2 below.
- **Operation Control Systems – Railway Undertaking (OCS-RU):** contains the trackside components that supervise the train missions, exchange information, perform diagnostics, configuration, and Maintenance, and even support remote driving which is mandatory for trains running under ATO GoA 3 to 4.
- **Physical Train Unit Operation Systems (PTU-OS):** contains among others the functional components of the TA, the TCMS that provides functionalities such as remote control, traction and brake controls, Digital Automatic Coupling (DAC), TIM etc. The TCMS connects to the CCS-OB either through the TA or directly and provides a direct interface to the Isolation Management component (ISM) of the European Train Protection On-Board (ETP-OB).

[2] A Building Block is a sourceable unit of the CCS on-board system (hardware and/or software), having standardised functionality, standardised PRAMSS requirements, standardised interfaces (on all OSI Layers) towards other building blocks and/or external systems [31].

- **Trackside Systems & Environment (TSE):** includes any trackside national ATPs, other trains (OTR), Eurobalises, Euroloop, and environment including PTUs and light signals.
- **Human Actors (HUA):** includes drivers, onboard staff, technicians etc.
- **Maintenance Equipment (ME):** includes the maintenance terminal (MNT) which can be a laptop connected through the Ethernet Consist Network (ECN) or ECN gateway to perform maintenance tasks on all the CCS-OB components.
- **Other Systems:** includes Time Service (TS) for time synchronisation and Augmentation (AUG) for improving the positioning system's performances using external information through a terrestrial dissemination service.

Within the CCS-OB, the European Train Protection On-Board (ETP-OB) is an important building that implements the on-board ATP part of the ETCS excluding functions with independent lifecycles (e.g., connectivity, localisation, etc.). As shown in 25, the ETP-OB block contains several functional components such as [31]:

- **Vehicle Supervisor (VS):** responsible for computing location-specific speed limits utilizing various inputs and activating the braking system when the speed limit is exceeded. It receives the movement authority (MA) from the trackside and reports the train position (TPR) back.
- **Euroradio Gateway (EGW) & Euroradio Safety (ERS):** acts as the gateway between the safe and the external, non-safe entities (e.g., On-Board FRMCS) and provides the appropriate safety integrity level (SIL) to the overall system.
- **Mode and Level Manager (MLM):** ensures that the proper ETCS mode and level are active and manages the transitions from one mode or level to the other.
- **STM Controller (STMC):** interacts with the national ATP systems and enables an automatic transition from ETCS to the national ATP system and vice versa while the vehicle is driving.
- **Physical ETCS Transponder Service (PETS):** reads the ETCS telegrams from the trackside installed infrastructure (Eurobalise and Euroloop) and forwards them to the CCS On-Board applications.
- **Cold Movement Detection (CMD):** a vehicle-based function that detects if the train has moved while the CCS-OB system was powered off.
- **Isolation Management (ISM):** allows the isolation of one or multiple ATP systems and informs the PTU-OS accordingly.
- **Trackside Condition Services (TCS):** in charge of managing the trackside condition information received from balises, Radio In-fill Unit (RIU), or RBC. It calculates the remaining distance to specific trackside points and triggers the appropriate actions according to the location.
- **ETP Repository On-Board (EREP-OB):** includes data storages for saving both operational data that has no relevance for long-term and static & semi-static configuration data.
- **ETP Data Recording On-Board (EDR-OB):** includes the Juridical Data Writing (JDW) and the Diagnostic Data Writing (DDW) components.
- **KMAC Services On-Board (KMAC-OB):** responsible for managing the authentication keys needed to establish a safe connection between the on-board and trackside entity.

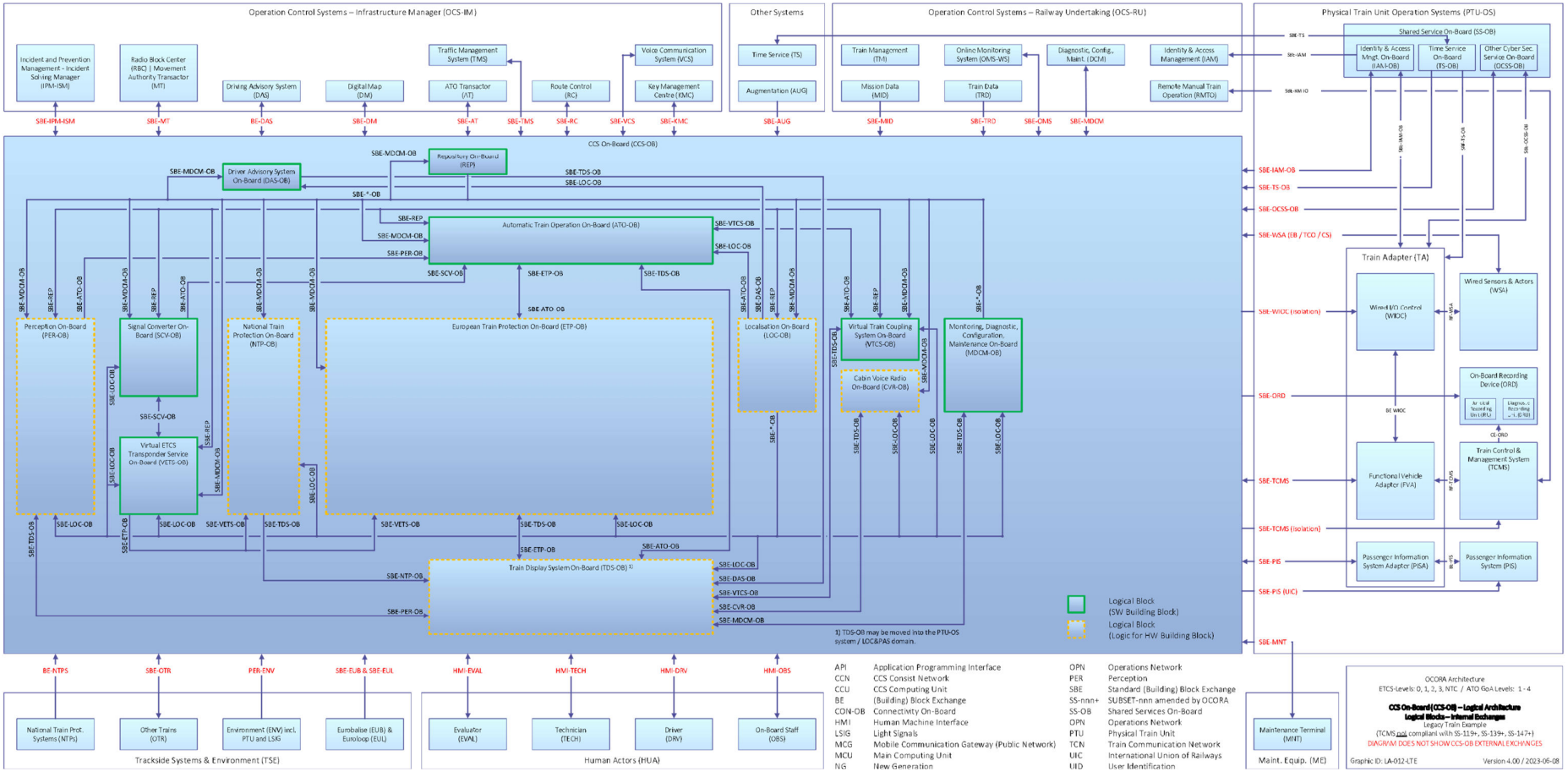

Figure 22: OCORA CCS On-Board (CCS-OB) – Logical Architecture depicting internal block exchanges for legacy trains. **[31]**

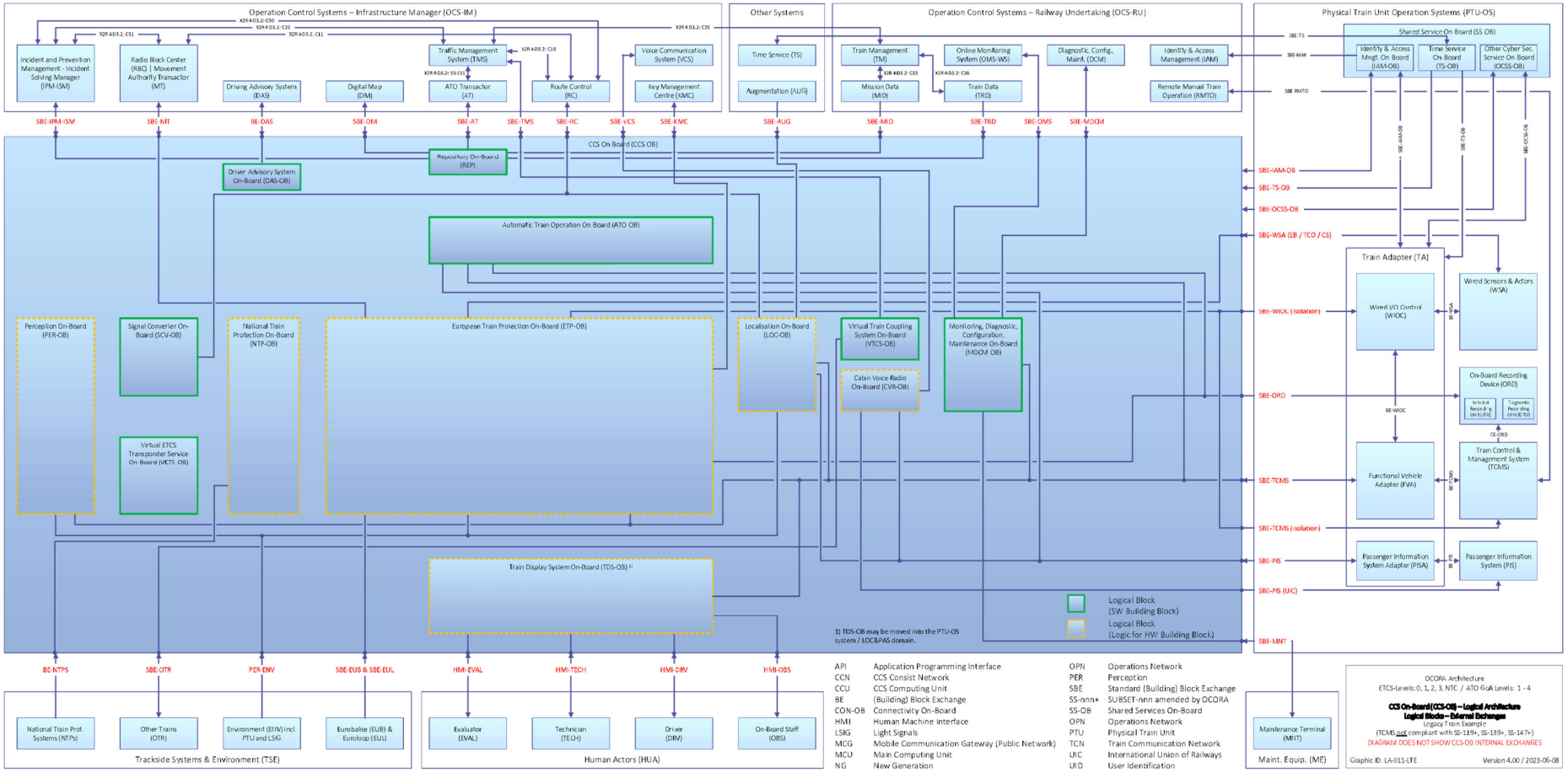

Figure 23: OCORA CCS On-Board (CCS-OB) – Logical Architecture depicting external block exchanges for legacy trains. **[31]**

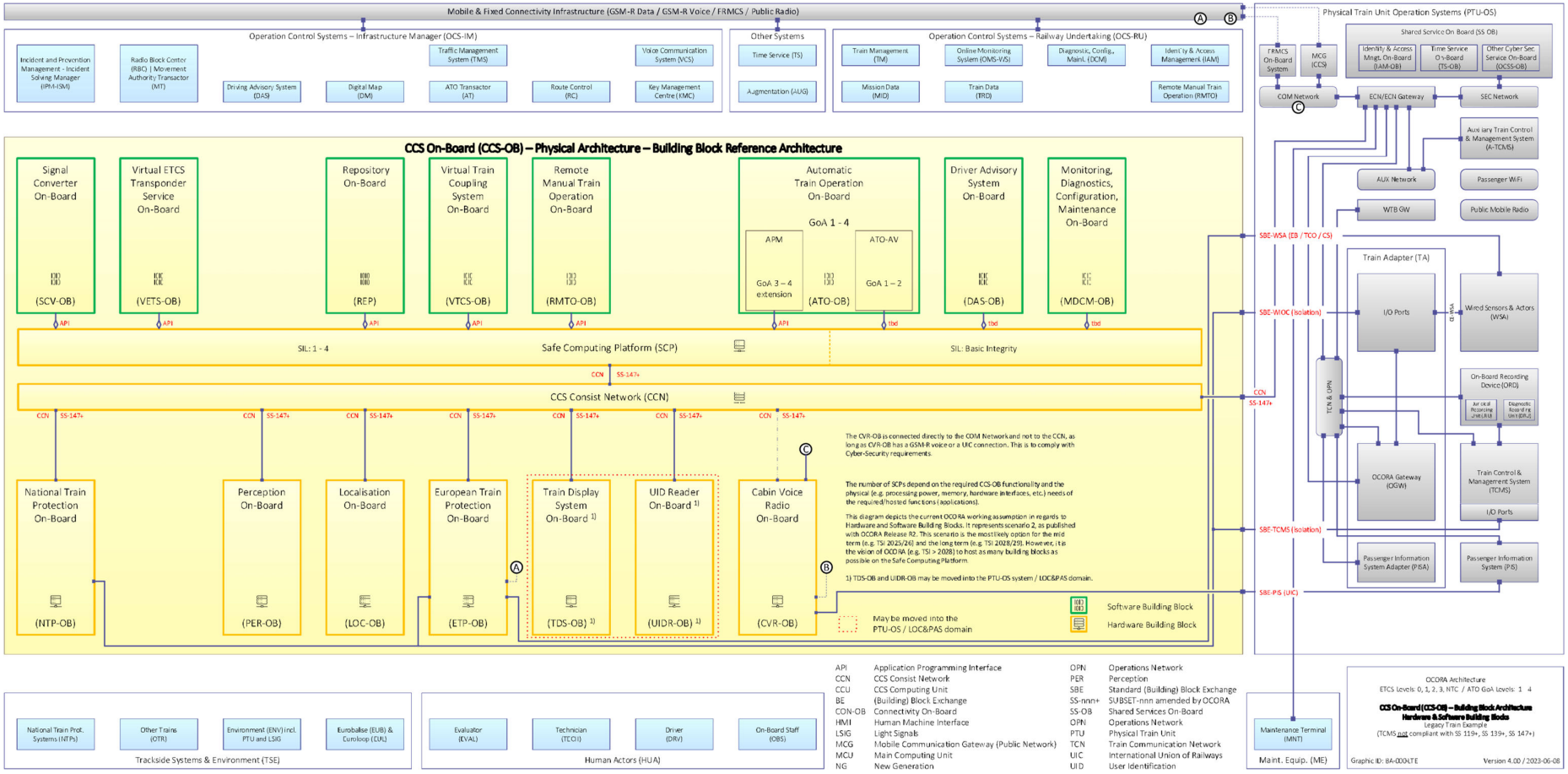

Figure 24: OCORA CCS On-Board (CCS-OB) – Physical Architecture with software and hardware building blocks for legacy trains. **[31]**

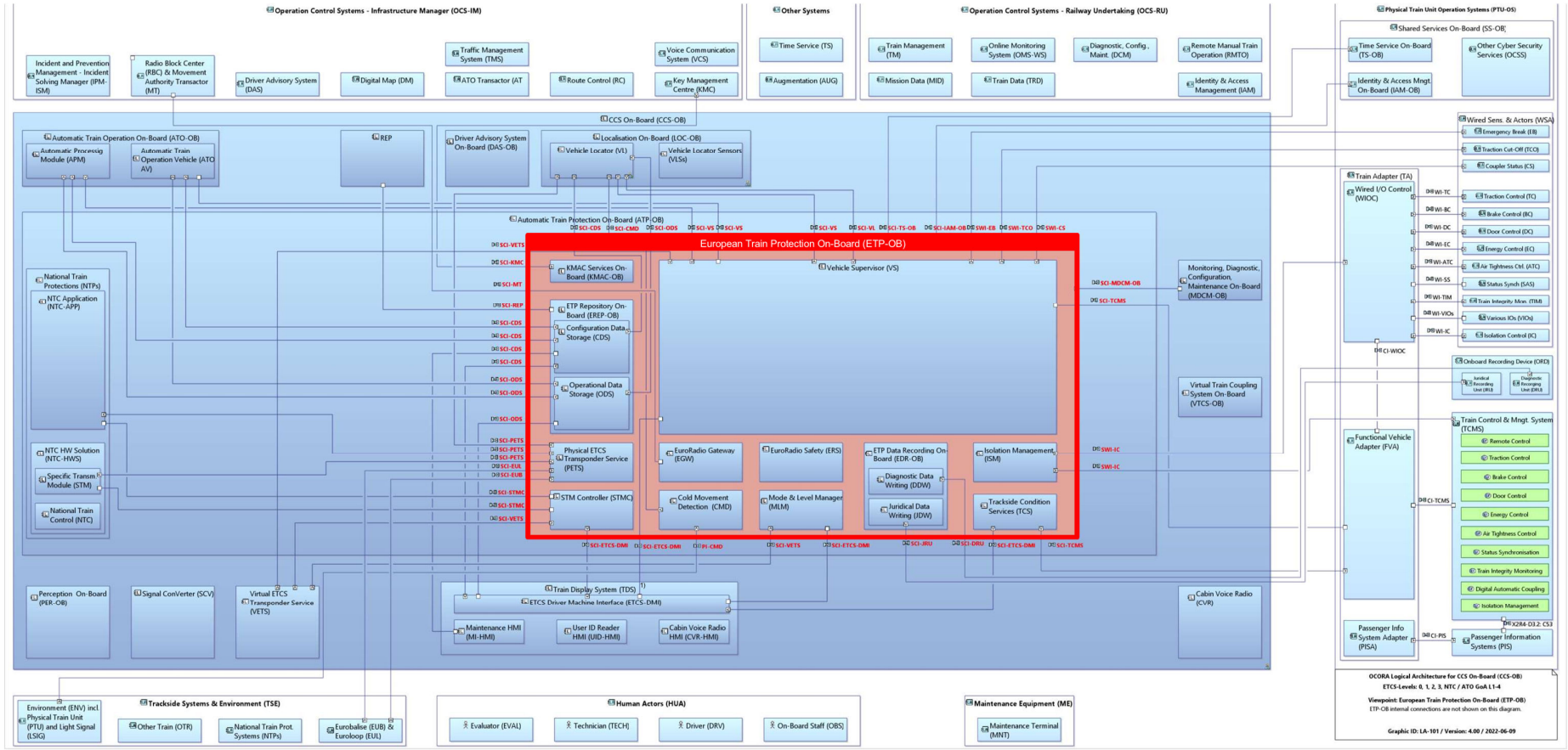

Figure 25: OCORA CCS On-Board (CCS-OB) – Functional components and interfaces of the European Train Protection On-Board (ETP-OB) **[31]**

In addition to ETP-OB, the ATO on-board (ATO-OB) is another important building block that is deployed on every OCORA-based CCS-OB system in need of ATO GoA 2 to 4 functionality. The ATO-OB block contains two functional components:

- **Automatic Processing Module (APM):** takes over the roles of the driver and the train attendant in case of an incident such as monitoring alarm signals and derailment, changing the running direction, managing the supervision status etc. It manages the mission execution, performs safe reflexive and evaluated reactions, and follows the safety protocols in cooperation with IPM-ISM.
- **ATO Vehicle (ATO-AV):** automatically controls the train's movements such as regulating the traction and braking, stopping at the desired location, managing the initial traction etc. The ATO-AV receives the ATO journey profiles from the Train Management (TM) subsystem in the OCS-RU actor group via the ATO Transactor (AT) subsystem in the trackside [5].

Additionally, with inputs from X2RAIL-3 [24], OCORA R4 introduces a Virtual Train Coupling System On-Board (VTCS-OB) building block in CCS-OB architecture that is expected to provide all the functionality needed for trains to drive in a virtual coupling mode. The interactions of the VTCS-OB with other CCS-OB internal blocks and external actor blocks according to OCORA R4 are summarized in Table 2. It is important to note that according to the working assumptions of OCORA, the VTCS-OB interacts with TIM, TCMS and ETP-OB through ATO-OB.

As mentioned in [30], the European railway community has chosen ATO over ETCS to be the preferred solution for implementing ATO in heavy rail environments, where ETP-OB is the primary ATP. Therefore, OCORA R4 as a baseline for CCS-OB may require adaptation of the VCTS system architecture [24] to coexist with ETP-OB that provides train interfaces to VTCS-OB. In a hypothetic VCTS over ETCS scenario, the VTCS-OB subsystem in the leading consist can be tasked with generating and communicating the ETCS specific movement authorities (MAs) to all the trailing consists by knowing their accurate positions so that the ETP-OB could still provide the ATP functionality to the trailing consists during VCTS missions without requiring to be disabled.

Blocks interacting with VTCS-OB	CCS-OB internal block	External block
Train Display System On-Board (TDS-OB)	X	
ATO on-board (ATO-OB)	X	
Repository On-Board (REP)	X	
Monitoring, Diagnostic, Configuration and Maintenance On-Board (MDCM-OB)	X	
Localisation On-Board (LOC-OB)	X	
Traffic Management System (TMS)		X
Other Trains (OTR)		X

Table 2: VTCS-OB interactions with internal and external blocks

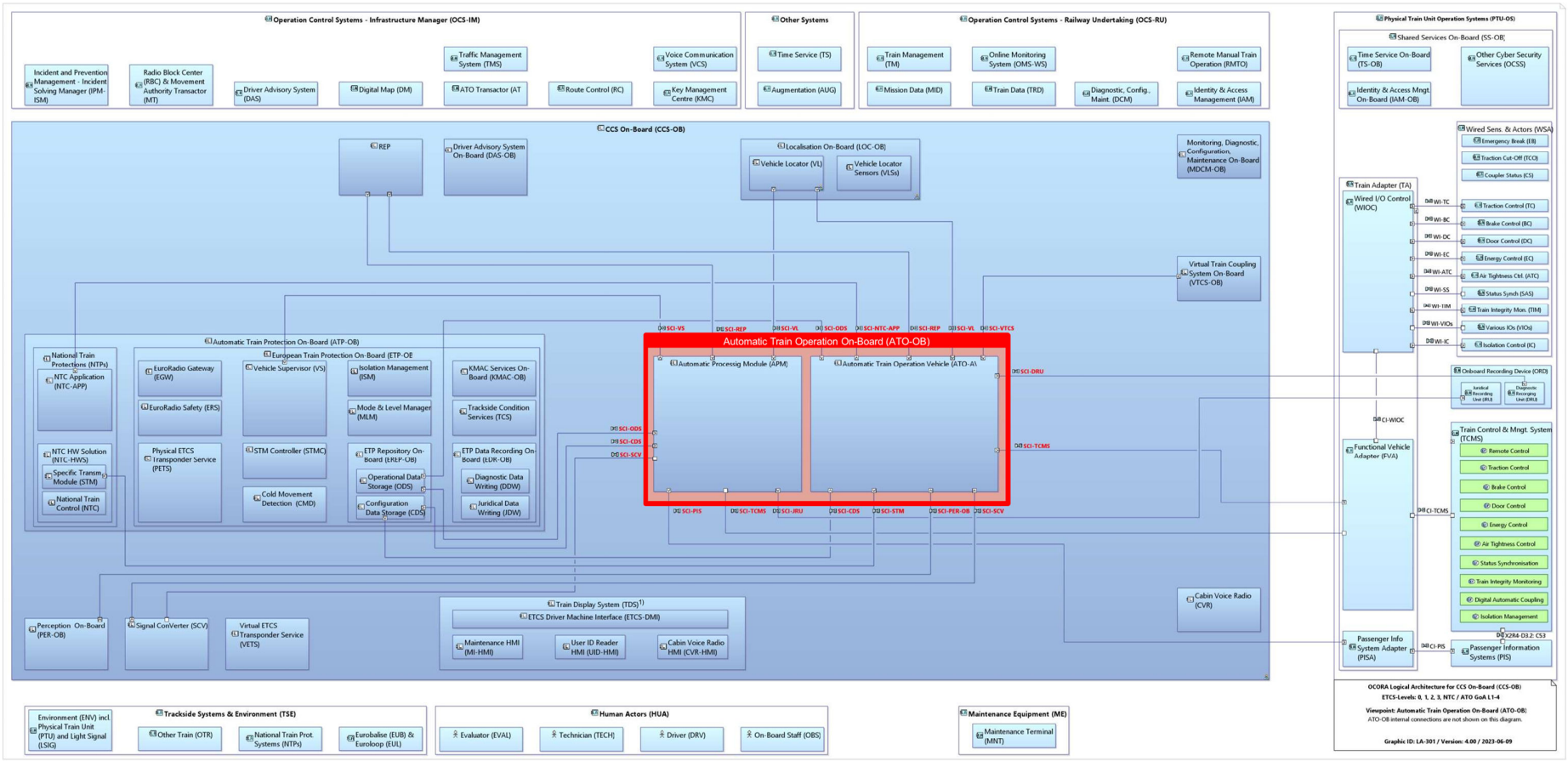

Figure 26: OCORA CCS On-Board (CCS-OB) – Functional components and interfaces of the Automatic Train Operation On-Board (ATO-OB) **[31]**

3.4.1.2 Reference CCS Architecture (RCA) for trackside CCS

The development of RCA was started in July 2018 with a memorandum of understanding by the EULYNX Consortium and the ERTMS Users Group (EUG) [32], predominantly consisting of infrastructure managers across Europe. RCA defines important interfaces needed to increase the modularity and reduce the life cycle costs of the CCS system. The RCA's scope is limited to the core functionality and interfaces of the trackside safety part of the CCS. The RCA target picture consists of radio-based communication between the onboard and trackside subsystems without lineside signals. To facilitate this, all the rolling stock running over intended lines will need to have the radio-based ETCS capability before the implementation of RCA trackside systems. OCORA presents an approach of achieving cost-effectiveness with the RCA infrastructure by providing a roadmap towards managed migration of the rolling stock.

The most recent documents from the RCA Baseline 1 Release 0 (BL1 R0) describe the Minimum Viable Product (MVP) of RCA. This BL1 R0 is planned to be the last release for RCA and the corresponding MVP results are planned to be integrated into the System Pillar (SP) [33]. An overview of the RCA trackside subsystem architecture along with the CCS-OB subsystem architecture is shown in Figure 27. Note that the CCS-OB subsystem architecture considered in RCA BL1 R0 is OCORA release R2 and looks substantially different to the OCORA release R4 considered in this document. For example, the Digital Map Repository On-Board (DREP-OB) referenced in RCA BL1 R0 is substituted by the Repository On-Board (REP-OB) subsystem in the OCORA R4.

The RCA architecture is divided into distinct architectural layers and the subsystems are assigned to exactly one layer. The Plan Implementation Layer obtains operational plans from the external Planning System (PAS) which oversees the entire schedule within the Area of Control. This layer executes the plans by generating discrete control commands and reports the state of the execution of the plans back to the PAS. This layer does not replan the schedule or perform conflict resolutions, as those responsibilities are handled by the PAS. The safety control layer maintains the railway's safety by validating commands in accordance with the current railway state. It permits validated commands to reach the Object Abstraction Layer and responds to any unsafe states of the railway. This layer executes combinations of logical functions and implements rules based on strictly abstract representations of real-world elements.

The object aggregation layer distributes and disaggregates abstract object commands to abstract device commands, and aggregates current states from abstract devices into abstract objects. Meanwhile, the device abstraction layer translates between commands and current states of the abstract devices, and those of specific devices. The device control layer is responsible for translating specific device commands into physical output for the controlled device. Additionally, it monitors and reports the state of the controlled device to the object aggregation layer. The generic function layer provides common capabilities needed by logical components in more than one of the other layers.

As shown in Figure 27, the RCA subsystems within these architectural layers include [34]:

- **ATO Transactor (AT):** distributes ATO journey profiles to the ATO-OB within each PTU. It provides status information and execution progress in the form of a Status Report Packet (STR) received from the ATO-OB.
- **Fixed Object Transactor (FOT):** translates between the abstract objects and the device-specific commands used by the Device Control Layer and vice versa for the subsystems:

- *Point (P):* used to control and monitor the Point Machines of moveable elements.
- *Level Crossing (LC):* protects the crossing area of rails and vehicles through its Level Crossing protection facility.
- *Generic IO:* used for integrating other safety-relevant systems.
- *Train Detection System (TDS):* monitors the vacancy and occupancy status of TVP sections (Track Vacancy Protection sections).
- *Light Signal (LS):* refers to stationary signals at the track, which can be set and show the visual signal aspect based on a command or a safety-related reaction.

- **Mobile Object Transactor (MOT):** functions like FOT by facilitating the translation between the abstract objects and the device-specific commands, but for location devices such as:
  - *Mobile Object Locator (MOL):* provides the position of a track bound (such as PTUs) or non-track bound (such as authorised trackside persons) movable objects.
  - *Person Supervisor & Locator (PSL):* provides warnings and protection from approaching movable objects along with information about their location on the railway network topology received from the subsystem MOL to trackside persons.
- **Movement Authority Transactor (MT):** translates commands and state feedback between the device-specific track-train message set and the abstract objects used beyond the Object Abstraction Layer. Among others, it translates from the Movement Permission (MP)[3] to the Movement Authority (MA)[4] for ETP-OB and from train position reports (TPR) to localisation report events for object aggregation.
- **Object Aggregation (OA):** distributes abstract commands to the relevant transactor subsystems in the Device Abstraction Layer and aggregates states from subsystems in the Device Abstraction Layer into abstract representations of the railway operation's state. It continuously provides the abstract railway operation's state to the Safety Logic subsystem.
- **Safety Logic (SL):** responsible for safe movements within a defined Area of Control (AoC). It evaluates requests for state changes in a Drive Protection Section Group (field element) and movement permissions by comparing safety parameters from the railway operation's state with predefined safety rules. Once confirmed as safe, SL grants the request and issues it as a command to the respective transactor.
- **Safety Manager (SM):** continuously supervises the operating state within the AoC, identifies hazardous conditions and initiates safety measures by issuing appropriate commands.

[3] A Movement Permission (MP) is an authorisation for a particular track bound movable object to move in a defined direction, with a defined maximum speed profile, along a defined path on the track network [137].

[4] A Movement Authority (MA) is permission for a train to run to a specific location within the constraints of the infrastructure [56].

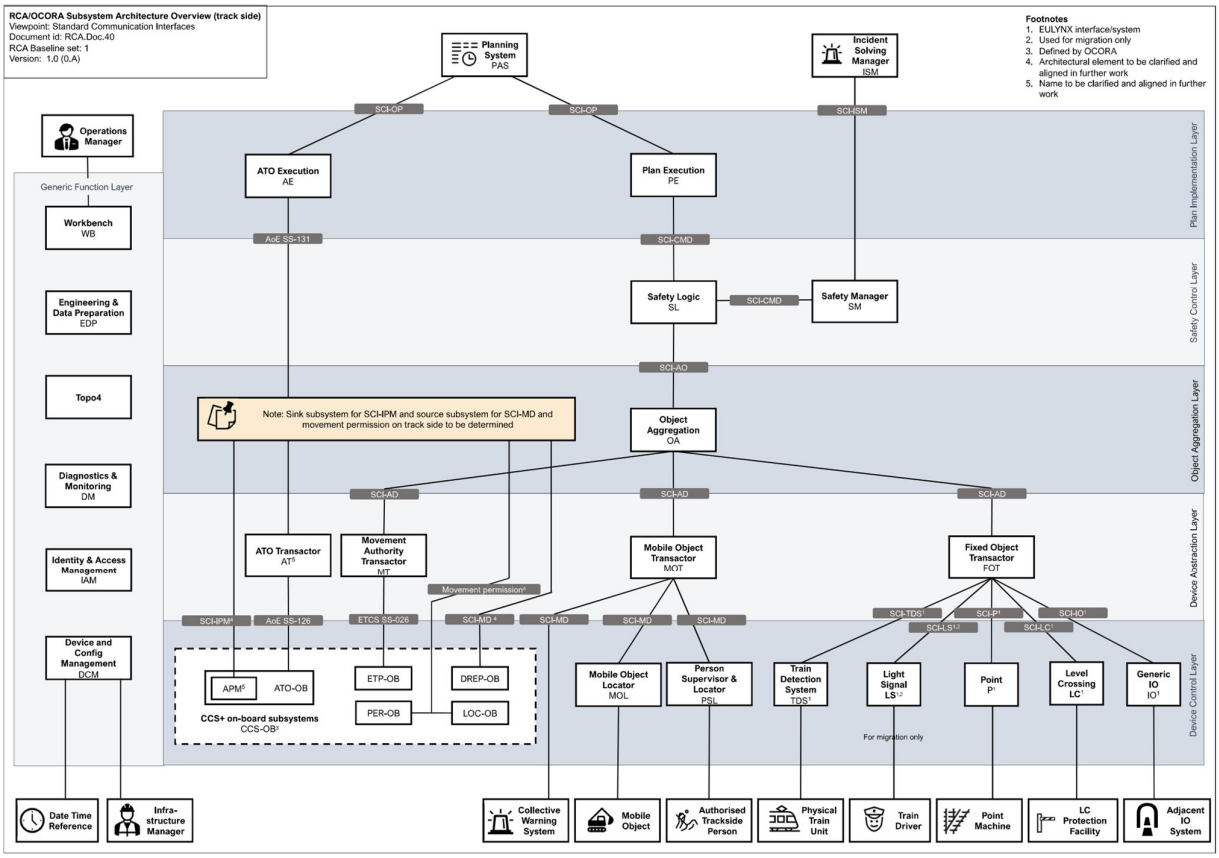

Figure 27: **RCA trackside subsystem architecture [136]**

- **Plan Execution (PE):** processes the operational plans sent by the external PAS and executes them by timely requesting movement permissions and intended state of field elements from SL. It receives the railway operation's state from the SL and reports it to PAS.
- **ATO Execution (AE):** translates the operational plans sent by the external PAS to ATO journey profiles (JPs) and provides them to ATO-OB via AT for timely execution. It also reports status reports (STRs) from AT as the Train Unit Reports to PAS. The same operational plan instance is also processed by the Plan Execution (PE) and is synchronized with the ATO execution on-board to secure the drivability of the railway network.

According to [35], the TMS is part of the external actor Planning System (PAS) and is outside the scope of RCA. It automatically plans and logs train movements as well as detects and resolves potential operational conflicts. Furthermore, the VCTS strategic layer functionalities could be integrated into the TMS [24]. As shown in Figure 23, the VTCS-OB interacts with TMS, but the trackside infrastructure that reliably exchanges mission data and status reports between the TMS and the VTCS-OB is still not defined. An approach similar to ATO can be followed within RCA, whereby the VCTS-related mission data and status reports exchange occurs through existing ATO trackside (ATO-TS), if feasible, or newly defined VTCS trackside (VTCS-TS) subsystems in the Plan Implementation and Device Abstraction layers.

Reliable communication between CCS-OB and CCS-TS is fundamental. The following section summarizes the current state and developments regarding railway communication.

3.4.1.3 Emerging System Pillar Traffic CS and Train CS

During the finalization of this document, first versions of the System Pillar's Traffic CS and Train CS specifications were circulated. Traffic CS and Train CS propose a more streamlined partitioning of CCS functionality than the current RCA and OCORA baselines. On the trackside, Traffic CS merges the traditional interlocking and radio-block-centre safety logic into a single European Trackside Protection System (ETPS), alongside a separate Plan Execution System (PES) that ingests Traffic Management System plans and issues fine-grained safety requests. By comparison, RCA's baseline still separates Plan Execution, Safety Logic, Object Aggregation and multiple device-transactor subsystems, each communicating via its own standardized interface.

On the onboard side, OCORA R4 breaks the two "super-blocks" ATP-OB and ATO-OB into internal modules (National Train Protection, European Train Protection, Automatic Processing Module, etc.). Train CS goes a step further by promoting several of these modules like NTP, ETP and the APM—into first-class, standalone logical subsystems. Each with its own standard interface, safety boundary and specification document, with the aim of easing independent procurement, certification and life-cycle management under a single System Pillar framework.

Once the Traffic CS and Train CS specifications are finalized, the VCTS technological baseline will be updated to reflect these new subsystems and interfaces. Further, EULYNX-style maintenance, diagnostics and security interfaces will be harmonized under the SP framework. Together, these changes are expected to improve modularity, simplify migration of legacy installations and strengthen multi-vendor interoperability without fundamentally altering the underlying ETCS-based moving-block and ATO GoA 2 architectures already in use. In summary, it is our understanding that the VCTS baseline presented here will require only minor updates—primarily to interfaces and module names—while its core functional design remains intact.

3.4.2 Communications

Railway communication systems are essential for the safety and efficiency of rail operations. Today's railway systems are characterized by centralized control which is reflected in centralized communications to the control centre responsible for a specific area. VCTS, however, has the potential to lead to more decentralized communication in rail operations through direct T2T communication, more localized data processing, and reduced reliance on control centres to perform local operational decisions targeting the VCTS.

In the following, existing systems like Eurobalise, Euroloop, and GSM-R are briefly explained. The next-generation Railway Mobile Radio (RMR) system FRMCS is introduced, and its role together with T2T communication as a backbone of VCTS is described.

3.4.2.1 Eurobalise and Euroloop

Eurobalises [36] are ground-based transponders that communicate pre-programmed information to the train onboard equipment. Some balises contain fixed information which can, e.g., be used for positioning, and balises that obtain current information from the signalling equipment. Each balise transfers a so-called *telegram* of either 1023 or 341 bits of size including overheads, which is very little information by modern standards. Nevertheless, the Eurobalise is a safety-relevant element of ETCS and thousands of them are in use in European railways today [37].

Euroloop is an extension of the Eurobalise system and provides continuous data communication between the track and the train. Euroloops are, however, not widely used within the EU railway, e.g.,

Germany is not using Euroloops at all [38]. Regulation (EU) 2023/1695 further states that Euroloops should not be installed on new lines, nor operated, except in specific cases (see 7.4.1 of the regulation).

3.4.2.2 GSM-R

GSM-R is a digital cellular communication system that was developed during the 1990s as a fundamental component of ERTMS to replace several incompatible analogue radio systems within railway applications [39]. GSM-R is based on the cellular standard GSM, the first second-generation standard (2G) which was introduced in 1990. Since then, communication demands have grown rapidly and today, GSM-R faces several limitations and challenges:

- **Limited Bandwidth and Data Capacity:** being based on older GSM technology (2G), GSM-R offers limited bandwidth and data capacity. This restricts the amount of data that can be transmitted, which is a significant drawback for advanced applications like real-time data sharing, high-resolution video transmission, or supporting Internet of Things (IoT) devices.
- **Cybersecurity Vulnerabilities:** older communication technologies like GSM-R are more susceptible to cybersecurity risks, and numerous security deficits have been shown for GSM [40]. Modern cyber threats lead to concerns about hacking, unauthorized access, and data breaches.
- **Quality of Service and Coverage Issues:** GSM-R users can experience quality of service issues, including signal degradation and coverage gaps, especially in remote or challenging terrains. This can lead to communication interruptions, which are critical for safety and efficient railway operations.
- **Interference and Capacity Constraints:** GSM-R networks can suffer from interference from public GSM networks, leading to potential communication disruptions. Additionally, as rail traffic increases, the capacity constraints of GSM-R become more apparent.

In conclusion, GSM-R played a pivotal role in modernizing railway communications. However, it now faces significant challenges and limitations that underscore the need for a more advanced communication system to meet the evolving demands of modern railway operations.

3.4.2.3 FRMCS

FRMCS is designed to be the future RMR system replacing GSM-R. It is being developed by the International Union of Railways and the European Union in close cooperation with important stakeholders [41]. FRMCS is expected to support all current GSM-R functionality and bring transformative change to railway communications. While FRMCS is designed technology independently, it will initially be based on 5G technology, which will ensure higher data rates, quality of service, and seamless integration of Internet of Things (IoT) devices.

3.4.2.3.0 Comparison to GSM-R

FRMCS's adoption is driven by the need for more robust and flexible communication systems in railways as it will offer significant advancements in the following areas:

- **Increased Performance:** FRMCS will provide significantly higher bandwidth, less latency and increased reliability. Mission Critical (MCX) communications essential for train movements and safety will be supported but even the transmission of vast amounts of data

that is essential to improve modern railway operations. This will facilitate advanced applications like real-time streaming for surveillance and extensive data sharing for predictive maintenance. Moreover, FRMCS will significantly improve non-MCX communications, such as seamless internet connectivity for passengers.

- **Enhanced Cybersecurity:** With increased connectivity, cybersecurity threats will expand. Therefore, FRMCS incorporates state-of-the-art cybersecurity measures including sophisticated encryption and secure communication protocols. Being based on 5G, FRMCS will benefit directly from targeted cybersecurity efforts from The European Union Agency for Cybersecurity (ENISA) [42] [43] [44].
- **Improved Coverage and Reliability:** Modern 5G technology like *MIMO* (combining multiple antennas on the transmission and receiving side) and redundancy on multiple layers (board, device, and network) will lead to improved coverage and reliability.
- **Reduced Interference and Scalability:** The use of additional frequency bands [45] dedicated to RMR will reduce interference. FRMCS' modular, software-based design and ability to allocate resources on demand enables increased flexibility to scale up communication networks. Furthermore, 5G's ability to prioritize certain traffic (quality of service) ensures that MCX traffic is delivered reliably in bottleneck situations.

FRMCS is further designed to be future-proof by following the evolution of radio technology, cost-effective by allowing seamless migration from GSM-R and interoperable among different railway networks and suppliers.

3.4.2.3.1 Relation to VCTS

VCTS will require T2G and T2T communication systems. Once implemented, it is expected that FRMCS will fully cover the T2G communication requirements of VCTS which include the formation and monitoring of platoons [25].

3.4.2.3.2 Current Status

Currently, FRMCS specifications exist to the extent that they are referred to by the CCS TSI, Regulation (EU) 2023/1695, as the successor to the currently employed GSM-R. The regulation also states, however, that they are incomplete, especially regarding tendering on-board equipment (see Appendix A of the regulation). Nevertheless, GSM-R products and services are currently guaranteed until 2030 only [46] which puts high pressure on the introduction of FRMCS. Thus, FRMCS can be expected to be widely available before VCTS is introduced. Within R2DATO, the efforts to introduce FRMCS are coordinated within WP25 "Connectivity Development – FRMCS".

3.4.2.4 Train-to-Train Communication

Previous work within Shift2Rail has been done on investigating potential technology for T2T communication, especially, in the X2Rail-3 and MOVINGRAIL projects that were part of TD 2.8 – Virtually- Coupled Train Sets[5]. Currently, there is no clear choice of technology available that can be considered as a technological baseline for VCTS [25] [47]. However, the VCTS system design and

[5] The public TD 2.8 deliverables are available online at:
https://projects.shift2rail.org/s2r_ip_TD_D.aspx?ip=2&td=aa1f0995-1402-4e7b-a905-49fba1bc6f71

interfacing in the following chapter is developed in close collaboration with R2DATO T48.4 “Technology development of Short Range Communications (SRC) and Relative Localisation (RL)”.

3.4.2.5 Conclusion

The landscape of railway communications is undergoing a significant transformation, driven by the evolving requirements of modern rail operations and the advent of innovative technologies. In the context of developing a new system like VCTS, the current systems of Eurobalises, Euroloops, and GSM-R should be regarded as legacy components. Therefore, the development efforts should primarily focus on FRMCS as the train-to-ground communication system. Eurobalises could be considered as supporting technology during a migration phase because of their widespread use. The choice of a train-to-train communication system is still an open question addressed in T48.4 of R2DATO.

3.4.3 Localisation

Precise and reliable localisation is an essential requirement for railways in achieving train separation and movement control. It plays an even more crucial role in enabling key emerging features such as ETCS L2 Moving Block, and VCTS which allow for optimized headways and increased railway capacity. Currently, the positioning of the train for signalling purposes in ETCS L1 and L2 are mainly based on the trackside infrastructure such as track circuits and if available, using on-board odometry which provides position reports based on distance travelled relative to the fixed reference positions of Eurobalises. However, the trend is gradually and increasingly moving towards on-board centric localisation using GNSS receivers along with data from different on-board sensors and digital map of network topology.

3.4.3.1 Eurobalise

As described in subsection 3.4.2.1, Eurobalises provide the possibility to send messages from trackside to on-board equipment. They contain geo-referenced positions along the track that can be used to reset the errors that propagate due to inaccuracies in on-board odometry sensors. For redundancy and to be able to transmit large messages, they are often grouped, consisting of one to eight balises [27]. The train position is computed by the odometer using the distance travelled since the last relevant balise group (LRBG) and it is reported to the RBC using Euroradio in ETCS L2 along with a confidence interval associated with odometer measurements. Currently, only physical balises are taken as reference locations to determine the actual train position.

3.4.3.2 Global Navigation Satellite System

Train positioning based on GNSS has been investigated by several projects [48], [49], [50], [51] and is seen as a potential alternative to resolve the dependency of today’s train positioning on using balises as a reference location. Using the virtual reference location concept [52] (also sometimes referred to as virtual reference point), GNSS is expected to achieve reduced deployments and maintenance of physical balises and improved odometry due to the possibility of more frequent resets of its confidence intervals than using only physical balises. Functionally a virtual reference location performs indistinguishably from a physical balise. They are logically installed at pre-determined locations along the track and when the position estimate of the GNSS matches the installed location, the position will be used as a reference.

Virtual reference location functionality coupled with GNSS face limitations in areas where satellite signals are obstructed, such as tunnels, hilly regions, and dense forests. Considering the high speeds at which trains operate, even a brief signal blackout lasting a few seconds contributes significantly to substantial uncertainty in GNSS position estimates. In such cases, physical balises remain necessary at specific locations where GNSS positioning alone cannot guarantee sufficient performance in terms of accuracy, availability, continuity, and localization integrity [53]. GNSS is also vulnerable to signal spoofing and jamming attacks and appropriate detection and mitigation measures must be addressed to safeguard the integrity of GNSS position estimates [54]. Integration of GNSS with other sensors and information sources (e.g., digital maps, a terrestrial dissemination service providing augmentation data) is crucial to fulfil the rigorous safety demands inherent in train control applications. Moreover, incorporating a satellite-based positioning system allows for not only precise and accurate positioning, but also train speed and acceleration.

As mentioned in [55], the accuracy of positioning has a crucial impact on VCTS performances. Within R2DATO, work packages 21 (WP21) and 22 (WP22) are focused on needs analysis and system architecture definition and RAMS analysis of ASTP system capable of providing accurate train location and kinematic data for all CCS components and various identified use cases. This ASTP system, along with RL being developed within R2DATO T48.4 is expected to meet the positioning requirements of VCTS and form the basis for VCTS implementation.

3.4.4 Train Integrity Monitoring

Railway operations such as route interlocking and ATP functions require the knowledge of both the train's front and rear ends to avoid collisions and derailments. By knowing an accurate front-end position of the train, the rear-end position can be calculated using the train length, but only if it can be safely asserted that the coupling between the wagons is intact and no wagon is "lost" along the track. "Train Integrity" is the notion of the level of belief in the train being complete and not having left coaches or wagons behind [56].

While the train front-end positioning is done by localisation subsystems described in subsection 3.4.3, the information about the rear end is today known by using trackside train detection systems consisting of track circuits and axle counters with an accuracy of the fixed block length. To achieve more optimized headways and increased capacity using concepts such as ETCS L2 Moving Block and VCTS, more accurate train rear-end positioning is essential. Within X2RAIL-2 [57] [58], an integrity concept has been developed with functional, architectural and interface specifications of the On-board Train Integrity (OTI) system for train integrity monitoring utilizing on-board systems. Within R2DATO, the OTI specifications from the previous projects are consolidated in work package 19 (WP19) [59] and a demonstrator‘s development is envisaged in work package 20 (WP20).

3.4.4.1 Axle counter

An axle counter is a device on the track that detects the passing of a train between two detection points (each end of the section). Each detection point comprises two independent sensors which not only increase reliability but also allow for the detection of the direction and speed of a train by the order and time in which the sensors are passed [60]. When a train enters a section, the axle counter registers each axle of the train and marks the section state as "occupied". When the train leaves the other end of the section, the axle counter once again counts every axle, and if the difference between the two axle counts is zero, the section state changes to "clear". This information is then utilized by trackside CCS to ascertain the train's integrity.

3.4.4.2 On-board Train Integrity (OTI)

The OTI is an on-board function that continuously monitors the completeness of the train while the train is in operation. According to OCORA R4 system architecture [31], the OTI functionality is part of an external TCMS subsystem outside of CCS-OB. In general, the function comprises an OTI Master module linked to ETCS and located in the front cabin, an OTI Slave module in the last wagon, and an on-board communication network for exchanging status data to assess the train's integrity status. The train integrity status can have three possible values: confirmed, lost or unknown. Different OTI product classes have been defined based on the communication technology employed [57]:

- **Product class 1:** trains equipped with a wired communication network where the integrity is determined based on the communication liveliness between the OTI modules in the front and rear ends of the train.
- **Product class 2:** trains equipped with wireless communication technology where the integrity is determined by comparing kinematic data of the train's front and rear ends.
- **Product class 3:** OTI Slave modules are installed in each wagon and the integrity is determined by verifying the separation distance between adjacent wagons. The modules communicate over a wireless on-board network.

In general, all classes of OTI systems are suitable for VCTS. However, class 2 and class 3 products are prone to longer reaction time to train integrity loss compared to class 1, primarily due to the nature of wireless communication. In VCTS, train integrity shall be monitored at two different levels: consist, and platoon. While *consist integrity* refers to the general notion of train integrity where wagons are mechanically coupled, *platoon integrity* means that the master train in the VCTS platoon shall be able to safely determine the position of the rear end of the platoon. The master train shall provide a Position Report message to the RBC including platoon integrity and platoon length information [61] so that the RBC can assign an EoA to the following train or platoon. A communication loss between the master and the slave trains is considered a loss of platoon integrity and is to be addressed in the same way as the loss of train integrity in a mechanically coupled train.

As highlighted in [55], the level of maturity of train integrity solutions is high and a number of candidate technologies have already been identified in [58]. To further facilitate the development of the OTI solutions up to TRL7, technological migration strategies are provided in [62]. Using the results from X2Rail-2 and X2Rail-4 projects, WP19 in R2DATO consolidated operational and functional requirements, and functional architecture for the train integrity and train length determination [59]. To ensure that different integrity and length determination technologies can interact, the concepts of "OTI Unit" (OTI-U) and "OTI Composition" (OTI-C) were introduced. Further OTI specification consolidation activities, its performance and safety analysis, and the development of demonstrators will be focused in WP20.

3.4.5 Summary

Within this subchapter, the technological baseline of various subsystems identified as significant for VCTS functionality is presented. Within the CCS domain, the existing ERTMS architecture is deemed inflexible and costly to update due to the persistence of legacy systems. Efforts are underway to establish a common SP architecture which is expected to be aligned with OCORA and RCA for onboard and trackside CCS, respectively. Due to the unavailability of architectural outputs from the SP at the time of writing in November 2023, these two architectures are considered to form the CCS

technological baseline for VCTS within this document. Since then, the SP has released a public concept for Traffic Control and Supervision (CS) as well as an architectural baseline for Train CS, which will require further analysis to assess alignment with the selected baseline.

The introduction of the VTCS-OB building block in OCORA release R4 stands as a pivotal step towards integrating VCTS concept within the system architecture. An approach similar to ATO is possible within RCA to exchange VCTS-related mission data between TMS and VTCS-OB, but these trackside subsystems and interfaces are yet to be precisely defined. In the implementation of VCTS, the existing communication infrastructure including Eurobalises, Euroloops, and GSM-R, should be recognized as legacy components. FRMCS, designed to replace GSM-R, promises higher data rates, superior quality of service, and seamless integration of IoT devices, aligning well with the requirements for forming and monitoring platoons within VCTS. As VCTS demands robust train-to-ground and train-to-train communication systems, FRMCS emerges as the primary focus for development, while legacy components like Eurobalises might play a supporting role during the transition phase. The choice of a T2T communication system remains an ongoing discussion, addressed within R2DATO T48.4.

Furthermore, the localisation and Train Integrity monitoring systems play a crucial role in enabling the functionalities of VCTS. While GNSS brings advantages such as virtual balises and improved accuracy, challenges like signal obstruction and security vulnerabilities persist, necessitating a hybrid approach that integrates GNSS with other sensors and information sources. Consequently, the ASTP system being developed in WP21 and WP22, along with RL technology being developed in R2DATO T48.4 forms the technological baseline for the localisation system for VCTS. For train integrity monitoring, in line with the trend shift towards on-board solutions, the OTI system developed within X2RAIL-2 forms the VCTS technological baseline. Whereas conventional trackside systems such as balises, track circuits and axle counters could be used for train positioning and integrity monitoring in degraded situations.

With this technological baseline, VCTS performs a leap towards the reduction of trackside systems in favour of onboard systems. We note that this shifts more responsibility for the safe operation of the railway from the IMs to the RUs.

4 SYSTEM DESIGN AND INTERFACING

4.1 INCORPORATION OF MAP-SUPPORTED MULTI-SENSOR LOCALISATION SYSTEMS AND METHODS

4.1.1 Section summary

The following material describes aspects of map-supported localization for VCTS. An overview of localization research in the rail domain is given in terms of stakeholders and literature. The relevance for VCTS is motivated. Localization and map activities within R2DATO are listed. Brief reviews of onboard sensors and systems and localization algorithms are provided. Finally, recommendations for future work are provided.
The chapter complements the respective localization sections in Chapter 3.

4.1.2 General remarks

4.1.2.1 On localization

The chapter uses the term localization. There are related terms that we do not distinguish when, for example, citing from the literate. Examples are the terms positioning (as in GPS) and navigation (as in GNSS). Important is that a vehicle perspective is assumed in which the algorithms can be executed on an onboard computer that has access to streams of onboard sensor and system data.
The material has relations to vehicle localization in general because (many of) the employed sensors and systems are also found in other domains. Examples include GNSS receivers and inertial measurement units (IMU) in road and rail vehicles. Similarly, the application of sensor fusion theory (for example, state estimation and Kalman filter algorithms to combine GNSS, IMU, and further sensor data) is not vehicle-specific.
Rail vehicle localization is relevant beyond VCTS. In fact, most automation and digital railway use cases rely on localization in some form. In contrast to the similarities to, say, road vehicle localization, there are many rail-specific aspects. On the one hand, rail vehicles are constrained to move along tracks in the railway network. With digital map data at hand, this information can be included into algorithms so as to achieve improved performance (accuracy, reliability, effects on train distances, etc.). This insight is key to the presented material. On the other hand, with the strict safety regulations, novel ideas and technologies are challenging to propagate, implement, or even test in the railway domain.
Localization for VCTS is an online application that relies on streams of sensor and system data. Results must appear instantaneously in real-time (with well-understood and well-restricted delays for the VCTS application). Terms that can appear in the context are online, real-time, but also onboard (to illustrate the short spatial and temporal distances between sensors and the processing unit that provides localization results). This is in contrast to offline localization on batches of previously collected data, a related problem that facilitates different algorithmic solutions. To highlight the contrast, terms that appear in connection with offline application can include batch processing, back-office, back-end (to emphasize the spatial and temporal distance between the sensors and the processing unit).
Map data is a key ingredient to improve the quality (accuracy and availability) of localization in the rail domain. Map data is a challenging topic in itself that can be understood in different ways, especially in combination with different sensor systems. To cater the core localization task with the most important and simple sensor systems with map-supported sensor fusion algorithms, the focus is on the geometric characteristics of the track network. Foremost, this includes the geographic locations of the tracks and information on the topology. The digital map needs to adhere to a number of requirements (accuracy, spatial resolution, completeness, common coordinate frames and units,

etc.). Furthermore, geometry information associated with the geographic locations can be exploited (for example, curvature, cant, elevation, azimuth). While this is a challenge to fully address, experimental data for first tests on sensor data can often be extracted from open map sources with limited efforts.
Map-supported localization can be understood in different ways. In the context of rail vehicles, the map should be regarded as an essential component of the localization algorithms and tightly integrated. It is not just an optional extra step in which localization results are refined using a map, e.g., by projecting position estimates onto the closest track (map-matching).
In addition to the above, localization must be seen in specific railway contexts. ETCS [63] should be mentioned with ECTS Level 2 with Moving Block (ECTS Level 3 in the past) as most relevant to VCTS. ETCS dictates requirements on the localization (both functional and non-functional). Whereas localization is now a part of the ECTS on-board unit, there are ambitions to replace this with an interface to a localization-focused on-board unit that can be accessed beyond ETCS. The architecture initiative OCORA addresses localization with such a separate on-board unit. Developments should be in line with this OCORA Localisation-Onboard [30]. Finally, the R2DATO project addresses localization with activities in dedicated work packages (WP21 and WP22) on ASTP. Onboard map data within R2DATO is addressed in a DR. WP27 is the associated work package. Last, there is a relation to relative localization concepts based on vehicle-to-vehicle communication (from consist to consists in VCTS-terms) in WP48.4.

4.1.2.2 Stakeholders and research landscape

The following paragraphs assume a European perspective for the sake of a compact presentation. It should be noted that there are relevant activities on all continents.
Meaningful research and development for railway localization must observe regulation and business aspects of the rail sector, and build upon existing results.
Railways are complex systems in many ways. There is the long history on the one hand and novel digital technology on the other. Long asset lifetimes and strict regulations are typical characteristics of the rail domain. Agile development of innovative (and therefore yet-to-be-perfect) solutions can be a challenge. There is a high level of standardization.
Diverse stakeholders influence the research and development.

- The European Union Agency for Railways (ERA) has the mandate to realize the interoperability of the rail system within the European Union (Technical Specifications for Interoperability, TSI) [64] [65]. Much time can pass before technical developments and potential solutions make their way to the TSI.
- Different political stakeholders on the European and national levels must address climate and society issues and therefore have an interest in a competitive and well-developed railway (digital, automated, efficient). Therefore, budgets are allocated to funding agencies (EUSPA, ESA) and initiatives (Shift2Rail, Europe's Rail) that have the mandate to finance suitable research and development. Furthermore, political stakeholders are involved in regulation and safety, for example, as national authorities.
- Railway and infrastructure operators are complex entities that act individually and as groups in different constellations. One the one hand, operators have the ambition to advance ETCS and other concepts. On the other hand, operators can be hesitant towards technical developments because of safety concerns and operational risks. An interesting initiative is the ERTMS Users Group (EUG) with participation by major European railway operators and the objective “to share experiences and to consolidate views” on ERTMS aspects. There are several working groups within the EUG dedicated to specific ERTMS topics. Of particular interest are the EUG Localisation Working Group (LWG) and the Reference CCS Architecture (RCA). Both develop and publish documents on technical issues (requirements, architectures, solution concepts).
- Large and established railway technology providers are involved in the technical development of railway technology. They need the business of railway and infrastructure

operators to sustain their existence. Hence, technical development must always have a business case for them. They are interested in the development of technical solutions and can benefit from research projects. However, onboard localization also aims at reducing infrastructure costs. Hence, the respective departments that develop solutions that rely on track-side infrastructure can have a separate perspective on onboard localization. The trade-off between onboard and infrastructure solutions needs to be carefully assessed without dismissing either. There are also smaller and more innovative companies that promote novel (on a spectrum from “completely new concepts” to “novel for the rail domain”) ideas and solutions. Some ideas from research can reach a next level more easily in startup companies.

- Universities and research institutes (for example, DLR) have the mandate to contribute to the development of the rail sector. The specific obligations are diverse (for instance, in terms of TRL). In comparison to technology providers there is an increased interest in publishing. The European railway research (localization in particular) appears more condensed in comparison to automotive research, which might be explained by the more agile character of the latter (vehicle life times, number of vehicles, development times, regulations).

4.1.2.3 Selected European research projects

The list of relevant activities is long and diverse in terms of funding volume, duration, stakeholders, and core topics. Here presented is a table with a selection of European projects from the recent past that have an obvious localization focus. The projects are grouped by the respective funding agency. GSA-related projects are put in the EUSPA category. Shift2Rail projects are put in the EU-Rail category. Where available, a link to the CORDIS portal is provided.

Project acronym	*Time frame*	*Agency*	*CORDIS-Link*
ERSAT EAV	2015-2017	EUSPA	https://doi.org/10.3030/640747
RHINOS	2016-2017	EUSPA	https://doi.org/10.3030/687399
STARS	2016-2018	EUSPA	https://doi.org/10.3030/687414
ERSAT GGC	2017-2019	EUSPA	https://doi.org/10.3030/776039
SIA	2018-2021	EUSPA	https://doi.org/10.3030/776402
CLUG	2019-2022	EUSPA	https://doi.org/10.3030/101082624
HELMET	2020-2023	EUSPA	https://doi.org/10.3030/870276
RAILGAP	2021-2024	EUSPA	https://doi.org/10.3030/101004129
EGNSS-R	2020-2022	EUSPA	-
CLUG-2	2023-2025	EUSPA	https://doi.org/10.3030/101082624
X2RAIL-2	2017-2021	EU-Rail	https://doi.org/10.3030/777465
GATE4RAIL	2018-2021	EU-Rail	https://doi.org/10.3030/826324
X2RAIL-3	2018-2021	EU-Rail	https://doi.org/10.3030/826141
X2RAIL-4	2019-2023	EU-Rail	https://doi.org/10.3030/881806
X2RAIL-5	2020-2023	EU-Rail	https://doi.org/10.3030/101014520
VOLIERA	2019-2022	ESA	-
AGIS4RAIL	2022-2024	ESA	-
EGNSS MATE	2023-2025	ESA	-

4.1.3 Localization for VCTS

VCTS relies on localization results. VCTS interfaces the onboard components of a localization onboard unit (LOC-OB in the OCORA context [54], ASTP as LOC-OB variant in the R2DATO context).

VCTS can in principle entail close distances between consists. Therefore, it can be regarded as more challenging than ETCS Level 2 with Moving Block. There is a shift from train set operation in absolute vehicle distances to operation in relative braking distances. A major difference is that VCTS will incorporate train-to-train (T2T) communication between vehicles (e.g., VCTS consists).

For further VCTS background the reader is referred to the respective sections of this report in Chapter 3.
In the VCTS operational layer, vehicle positions and velocities are required for control purposes. The thrust and braking actions of each consist need to be determined by a control algorithm so as to follow a dynamic reference trajectory (that can be derived from a relative distance to the adjacent consist) in position and velocity. For control purpose follow qualitative frequency requirements. The output data rates should be around 100 Hz or higher for position and velocity control of the consist.
In the VCTS tactical layer, the position and motion estimates of several vehicles in a VCTS are combined to gather the overall information and derive commands or reference trajectories for the individual consists. Coupling and uncoupling decisions that alter the train sets are met.
The VCTS strategic layer can use aggregated localization information to optimize on a higher level with the information from several train sets. Respective decisions and control actions can be made and passed on.
VCTS will not bring its own localization functionalities. Instead it must rely on localization information provided by a respective on-board unit.
With the importance of relative positions between the consists of a VCTS, respective solutions play a more important role. There are technological solutions for this, as demonstrated in R2DATO WP48.4. Whether these will lead to a separate onboard component for relative localization that can be accessed by VCTS, or whether relative localization will enter future onboard localization (LOC-OB or ASTP), remains to be determined.

4.1.4 Localization and maps within R2DATO

An overview of the ongoing activities in R2DATO is given based on the available deliverable reports at the time of writing. The reports that have been utilized are all classified as public according to the R2DATO grant agreement and will be accessible as download.

4.1.4.1 Absolute Safe Train Positioning

Localization in R2DATO is the core topic of WP21 and WP22 on ASTP. WP21 has consolidated the operational needs and system capabilities of ASTP among several operator, industry, and research stakeholders in the first project months. System requirements have been listed. WP22 focuses on a number of demonstrators to realize ASTP or parts of it using different approaches. It is planned to conclude with demonstrator assessment and TSI gap analysis. Not all deliverables and technical details are publicly available. The work is ongoing as this report is being finalized.
Insights from WP21 are listed in

- R2DATO D21.1 – Operational needs and system capabilities of an ASTP system (Use Cases). [66]
- R2DATO D21.2 – System requirements of ASTP system. [67]

ASTP is seen as technical enabler within R2DATO. It serves CCS and non-CSS systems. Hence, ASTP is the system for localization in VCTS. Current localization approaches for ETCS are reviewed as starting point for ASTP. Reference frames are defined. As reference position on a vehicle, a bogie frame is introduced. Train front end and train rear end positions are distinguished. A 3D position reference frame is used to cater for the absolute position. An attitude reference frame is used to cater for the vehicle orientation with respect to the 3D position reference frame. This appears in line with localization research without rail specifics. A 1D position frame (distance and track edge) is introduced for track-constrained position information. Confidence intervals are used to describe regions for the true train position, velocity, acceleration with a defined probability. Localization results are correctly referred to as estimated quantities (distance, position, velocity, etc.). Different messages for localization results are agreed (1D position with distance and track edge id, 3D position, train attitude). In addition to confidence intervals, covariance information is utilized to describe uncertainties in the localization results. The concept of relative position is introduced as scalar distance from a reference location. Here is a link to WP48.4 with relative localization of vehicles (and hence, the distance to a moving reference location). To cater for the safety, ASTP

introduces the concept of valid localization information from the ASTP perspective. Operational scenarios are listed with qualitative non-functional requirements on the localization results (e.g., low-speed and high-density scenarios with small headway require high accuracy). Scenarios are clustered into start of mission, shunting, moving, among other categories. Extensive environmental conditions are listed in which ASTP must be fully functional (weather and severe weather, lighting, tunnels, bridges, etc.). VCTS is listed among the ASTP users. DR is listed as source of map data for ASTP.
First insights from WP22 are listed in

- D22.1 ASTP Report on Common Overall Design and Architecture. [68]

D22.1 is an architecture deliverable for future ASTP. Not all demonstrators of WP22 adhere to this architecture yet. The connection to the digital register DR is underlined. ASTP goes beyond the ETCS odometry that provides relative position to a previously read balise. Safety considerations of the position estimates in ETCS dictate that the true position is within the given confidence interval. ASTP is a separate module from ETCS that provides higher accuracy and 3D position, among other quantities of interest. It is highlighted that the core of WP22 is demonstration rather than the development of a common interoperable solution. The future changes to ETCS to incorporate the proposed ASTP solutions is seen as future work. There are many different sensors in consideration. A list of minimum undeniable sensors and data sources includes GNSS (including EGNOS and augmentation), Inertial Measurement Unit (IMU), speed sensors, and map data. Balises and route information are mentioned but beyond the core information. The sensors and details of the demonstrators are given in several tables in D22.1. Block diagrams of the individual demonstrator architectures are provided. These differ considerably regarding the details on the actual combination or fusion of sensor data.
Specific map data is required for some approaches, including the magnetometer array approaches by DLR. Beacon-dependent UWB localization is investigated by CEIT. RF-ID tags are discussed. Cost reduction by reducing the number of balises is discussed. ASTP installation as a network access criterion for vehicles is discussed. Rail-specific aspects of EGNOS are described. Architecture suggestions are made and discussed. These show ASTP and ECTS as separate blocks. The deliverable concludes:

- ASTP shall provide an independently certifiable, interoperable constituent.
- ASTP shall provide a standardized “grey box” solution with an agreed minimum sensor configuration and further sources.
- GNSS will be an important component of ASTP.

4.1.4.2 Digital Register

R2DATO has a dedicated work package (WP27) on the DR for storing and distributing digital infrastructure and map data to several onboard applications (from traffic management to ATO to localization to perception, etc.). In the WP jargon the different applications are called domains. ASTP is one such domain. For localization in VCTS via ASTP the DR must be used as map source. WP27 has published openly accessible deliverables:

- R2DATO D27.2 – Specification of the Digital Register implementation(s) required in FP2-R2DATO. [69]
- R2DATO D27.1 – Set of requirements on the Digital Register in R2DATO. [70]

Initial requirements of DR are listed in D27.1, with the remark that the requirements are rather a first step than a complete set. An update on the requirements is planned for D27.3 in mid-2025. DR has an on-board system (DR-OB) and a track-side system (DR-TS). There are the notions of map data (static and detailed) and on-board map data (specialized form for a certain application). The concept of a segment profile is introduced as one-dimensional object that describes a single section of a track (with a start point, end point). The main purpose is said to be for ATO on-board operational speed profiles. However, the notion of a segment with points (as geographic locations) and along-segment values (e.g., distance-on-the-segment, track-geometry-value-on-the-segment, etc.) fits well

with map data used for localization. The overall architecture with DR-OB and ASTP as consumer (taken from D27.1) is given in the figure below.

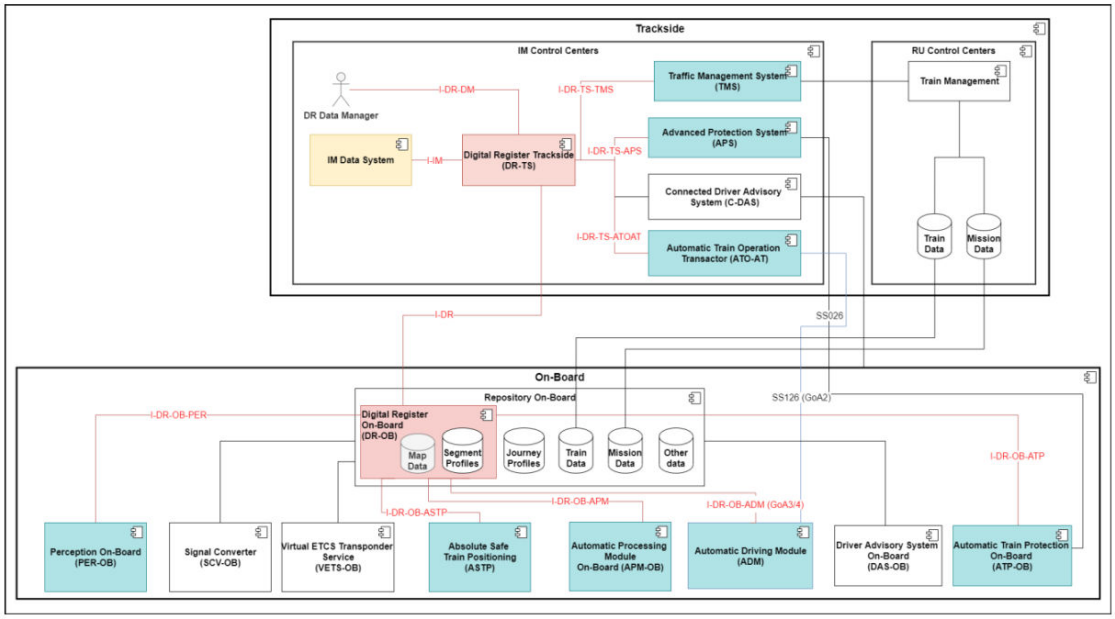

Figure 28: Architecture of the digital register **[70]**

D27.1 does not specify the domain data. That is, the specific form of the map data and requirements that come from ASTP are not given.
D27.2 specifies the architecture for DR and consuming systems such as ASTP. Several logical DR components are listed (DR validator, DR publisher, etc.). On-board maps as domain data for ASTP are not described in detail. Interface scenarios between DR and consumers are described on a higher level (domain data pull).

4.1.4.3 Relative Localization

R2DATO WP48.4 bridges communication systems and RL. For VCTS this is important as potential information source for controlling the distances between consists in the VCTS tactical layer.
There is a publicly available deliverable

- D48.4 Technology development of Short Range Communications (SRC) and Relative Localisation (RL) [71]

with much technical content on T2T and SRC with distances up to 250 meters. The VCTS relevance is elaborated as target application. Technical requirements on latency, reliability, packed size, communication range, and bandwidth are addressed. SRC is seen as important for RL because it facilitates the exchange of time-stamped data packets from which the distance can be calculated. Suitable communication standards are discussed. There is a lack of commercially available equipment. Therefore, project specific hardware is developed and employed. Field tests are planned and their preparation documented. Results will be included in D48.5.

4.1.5 Literature review

4.1.5.1 Information sources

From the complex stakeholder landscape follows that relevant information is found in diverse information sources. These include:

- Books and scientific conference and journal papers with a transportation or railway focus. In comparison to the automotive domain there are fewer articles on GNSS and localization in railway.
- Scientific literature with a GNSS or sensor focus. Many topics go beyond transportation. For example, interference has an effect on GNSS regardless of its specific application.
- Documents developed in different railway communities. Examples include reports from the EUG Localisation Working Group (LWG) or the architecture initiative OCORA.
- The research project landscape with deliverable reports. Not all results and findings are accessible. Relevant insights can appear only as side topics in a project. Hence, the probability of overlooking them is high. The research landscape is dynamic and it happens that project websites disappear. The CORDIS portal as repository for EU-financed projects is a long-term reliable source (objectives, partners, dates, deliverables).
- Sensor manuals, data sheets, software manuals, and similar documents can be relevant. Again, the environment is dynamic (product and software websites) and the relevant information might not be as accessible.
- CORDIS (https://cordis.europa.eu/) is a portal for information on projects by the European Commission (Horizon Europe etc.). It contains details on the partners, budgets, timelines, and collects the public deliverables and reports.

From the above view on the available information sources and stakeholder landscape follows: The field is complex. Condensing the information into few paragraphs is bound to leave gaps and over-simplify. There is much information available in diverse information sources. It is important to build upon such existing results. Because of the diversity it is difficult to address different stakeholders in a single place or format. Attempts to capture one overall “state of the art” are bound to be incomplete.

4.1.5.2 Books

The Springer Handbook of Global Navigation Satellite Systems [72], edited by Teunissen and Montenbruck and published in 2017, is an extensive reference on GNSS. It explains the different GNSS (GPS, Galileo, etc.), the underlying principles and theory (observation equations, solutions, PPP, RTK, etc.), and the challenges (interference, multipath, etc.) in great detail. Furthermore, selected applications (including a brief segment on railway) are provided.

Position, Navigation, and Timing Technologies in the 21st Century [73] is a comparable two-volume resource. It also covers mores recent developments (chapters on LEO navigation) and content beyond GNSS (chapters on laser, cameras, magnetic field sensors). The chapter [74] is dedicated to GNSS in the rail domain and ERTMS.

Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems [75] is a comprehensive GNSS reference. In contrast to the above it provides more background on inertial measurement units, sensor fusion, and Kalman filter algorithms.

GNSS for Rail Transportation [76] is an edited volume on the use of GNSS in the ERTMS ETCS context. Requirements from the railway application are discussed (SiL, integrity, confidence intervals, protection levels). The presented GNSS localization does not employ a full sensor fusion system.

Operating Rules and Interoperability in Trans-National High-Speed Rail [77] provides a detailed ERTMS background.

Intelligent Processing Algorithms and Applications for GPS Positioning Data of Qinghai-Tibet Railway [78] is an Asian case study, which has been published as book. It discusses GNSS aspects and also the use of map data.

[63] is a freely available book on railway signalling. Aspects of ETCS and other Automatic Train Protection (ATP) systems are explained.

[79] and [80] are comprehensive references on sensor fusion algorithms, including Kalman filters, particle filters, state space models, noise modeling, and Bayesian filtering.

[81] is book that covers the fundamentals of railway design (vehicles, tracks, from high-speed rail to trams).

4.1.5.3 Review papers and book chapters

[51] is a much recommended 2017 review paper on GNSS localization in the rail domain. It is related to the project Satellite Technology for Advanced Railway Signalling (STARS) and the deliverable [48]. Localization and the specific demands of the rail domain (ERTMS ETCS) are covered. Attention is dedicated to the use of GNSS augmentation with EGNOS. Limitations and GNSS challenges (local multipath, local interference) are provided. Safety aspects are discussed (GNSS integrity, RAIM, SBAS and GBAS, protection levels, redundancy, fault detection and exclusion). The project landscape is summarized up to 2017.
[82] is a similar survey that discusses projects, applicable sensors (GNSS, IMU, speed), algorithms, and results.
[74] is a book chapter in [73]. The general motivation of localization is presented along ERTMS ETCS concepts. The focus is on virtual balise (VB) concepts. Here, GNSS is suggested to be used in specific locations and included into a localization solution similar to a regular balise. As an advantage, only minimal changes to the ETCS localization (balises and odometry) are necessary. Several safety aspects are discussed.
[83] does not provide material on localization. However, as railway chapter of the Springer Handbook of Mechanical Engineering it can provide a good starting point for vehicle and infrastructure background. For instance, track geometries (curvature, radius, gradient, cant) or RAMS aspects (Reliability, Availability, Maintainability, Safety) are discussed.

4.1.5.4 Selected PhD theses

Plan [84] is a PhD thesis from 2004 (written in German) that already describes many interesting aspects. The challenges of shunting and industrial railways (bad GNSS reception, agile motion) are explained. Sensor concepts and the use of map data are discussed.
[85] is a comprehensive thesis on map-supported multi-sensor localization. Also map generation from sensor data with SLAM approaches is covered. Details of the specific use of map data are discussed. A rich background on sensors is given, including GNSS and IMU, but also magnetic field measurements. Relations of the IMU signals to track features (curvature) are discussed. Furthermore, relations between the velocity and the IMU spectra in the frequency domain are explored. Sensor fusion approaches are discussed from a Bayesian perspective. Two main localization approaches are contributed. First, a map-supported particle filter (PF) approach is given in which the particles populate the relevant track hypotheses in the track network. The approach is also covered in a journal paper [86] listed below. Second, a filter bank variant is suggested in which several track hypotheses are treated in parallel. The approach is termed multiple hypothesis tracking (MHT) by the author, but bears little resemblance to the MHT problem in the tracking literature (tracking of an unknown number of targets or objects without access to their onboard data; involves data association, missed detections, false alarms). In order to avoid confusion, the name filter bank should be preferred. A probabilistic approach with relation to the likelihood computation in a PF is presented to assess the performance of each filter in the filter bank. Experimental results on real data are described in the thesis.
The 2022 PhD thesis by Winter [87] is written in German. The author has published a range of papers that are contained and presented in a unified manner. Safety critical localization with onboard sensors and systems (GNSS, IMU, velocity) is addressed, with pointers to the strict accuracy, integrity, and availability requirements. The contributions include novel sensor fusion algorithms, an approach to derive map data from onboard data, and the evaluation of both on actual measurement data. Data and software were made available by the author. Valuable context on specific GNSS, IMU aspects, but also algorithmic details on motion detection, calibration, and filter initialization are described exclusively in the thesis and not published elsewhere. The proposed localization filter utilizes the fact that there are only three different types of railway track segments (straight, curved, and transition segments). By estimating the currently used track segment type, information on the track-constrained vehicle motion can be exploited without the need for actual map data. An interacting multiple model (IMM) filter is proposed in which the track segment types determine the

mode variables. The state vector includes horizontal position, driven distance, scalar velocity, scalar acceleration, yaw angle, and yaw angular rate. GNSS measurements are assumed to provide horizontal position, speed, but also the course angle. From IMU the longitudinal acceleration and the turn rate about the vertical axis are included. Motion and measurement model details are provided for the aforementioned track segment types. A fallback solution is provided for occasions in which the track segment cannot be classified well enough. The approach is shown to provide increased accuracy in comparison to a map-less GNSS and IMU localization extended Kalman filter (EKF).
The 2017 PhD thesis by Stein [88] is a bit beyond the scope of this report. The focus is on lidar (light detection and ranging) in the rail domain. Nevertheless, it is relevant because it shows the relation to further information sources that are likely to be used for perception in ATO efforts.
Several German PhD theses from the Karlsruhe Institute of Technology (KIT) are relevant. [89] discusses eddy current sensors, GNSS, IMU, and map-matching approaches. [90] discusses eddy current sensors, speed and distance estimation, and switch detection in the eddy current signals. In this context, also probabilistic localization in topological maps is described. [91] describes SLAM approaches and filter bank localization with several hypotheses. [92] describes the development of a difference inductance sensor.

4.1.5.5 Selected patents and journal papers

[93] is an example of an early patent with GPS use in the rail domain. In addition, trackside transponders and wheel tachometers are incorporated.
An early example of map-supported localization in the rail domain is [94]. It does not employ GNSS. Instead, it merely relies on a yaw gyroscope (for turn rates about the vertical vehicle axis) and a tachometer (for speed). The “map-matching” in the title refers to finding correspondences / maximizing correlation between gyroscope measurements and features of map segments. Hence, the approach is a first example with requirements on the map. Namely, it must be ensured that the respective features can be queried from the map data in good quality.
[95] addresses wheel speed sensors and slip-and-slide phenomena and proposes a Kalman filter approach to obtain improved distance estimates.
[96] utilizes a specialized eddy current sensor for velocity estimation and turnout detection in combination with a topological map of the network. A particle filter (sequential Monte Carlo, SMC) for a proposed hidden Markov model (HMM) is used.
[97] describes a SLAM approach for the rail domain. It employs the data of an integrated navigation system with GPS and IMU.
[98] uses GNSS and velocity sensors (wheel encoder, Doppler radar, or eddy current). Relevance for the virtual balise idea is stated. Map information is included (geometries, topology). Bayesian modeling and Kalman filter are employed in combination with map data. The algorithm includes hopping along tracks to cope with different path hypotheses. Experimental results (for road and rail data) show improvement over simple GNSS map-matching. IMU data is not considered.
[99] describes RAMS and receiver performance aspects for GNSS localization in the rail domain. Sensor fusion is not addressed explicitly.
[86] describes a particle filter localization approach based on probabilistic modeling and advanced map information. Due to the stochastic nature of the PF there is randomness in the results. Furthermore, challenges with the high-dimensional state space (curse of dimensionality, particle degeneracy) can be a risk for PF in general. The material is also addressed in the author’s PhD thesis monograph above.
[100] investigates KF-based GNSS for localization in ETCS in terms of safety by providing a risk analysis.
[101] uses BeiDou as GNSS source. Fusion with IMU and velocity sensors is discussed. Subsequent map-matching in mostly single-track scenarios is proposed. Kalman filters are employed. Experimental results are given.
[102] complements GNSS/IMU integrated navigation with position information from turnout detection in lidar data.

[103] addresses GNSS jamming detection in a virtual balise setting with a simulation study.
[104] discusses a solution for GNSS and IMU integration and subsequent map-matching. Different nonlinear Kalman filters (EKF and UKF) are utilized and tested. Experimental results are provided.
[105] describes a KF bank approach for localization with GNSS, velocity sensors, IMU, and tightly integrated map data. Several path hypotheses (sequences of tracks) are considered in parallel. Paths are managed (by trimming to keep only the relevant tracks underneath the vehicle, by extending to ensure that the paths are long enough and that newly generated hypotheses are included at switches). On-path KF are fed with the available measurements at each time step. The KF return measurement residuals (or related quantities) that are then used for performance evaluation, finding the best hypothesis, and removing no longer used or badly performing paths. The approach is central to the EGNSS MATE project. A more technical publication is in preparation by the author.

4.1.5.6 Selected conference papers

[106] builds upon the idea to connect the IMU turn rate about the vertical axis with the curvature of the track (looked up in a map database). It is shown that this can provide the path after a switch has been passed.
[107] presents on-board localization in the PTC context (positive train control, the US train protection system and cousin to ETCS). Fusion of GPS and IMU using an extended Kalman filter (EKF) is proposed. Map data can be incorporated as “subsequent refinement”. No algorithmic details of the EKF are presented. From the provided information (choice of state vector with 3D position, velocity, acceleration, IMU bias and drift values) can be inferred that no railway-specific filter or motion model has been employed.
[108] is a map-supported offline approach that uses path estimation and on-path Kalman filters and Rauch-Tung-Striebel smoothers. The concept of a railway path is introduced here.
[109] proposes an interacting multiple model (IMM) approach using EKF for the fusion of GNSS and other sensor data. The mode variables correspond to the track type (straight, curved, transition segment). Thereby, map information can be used without having access to a map data base.
[110] provides an open data set from the DLR research vehicle RailDriVE that can be used to evaluate algorithms for localization at low speeds.
[111] employs a novel difference inductance sensor (DIS) that measures ferromagnetic quantities of the track underneath the vehicle. From the DIS acceleration, velocity, and fingerprint information can be obtained. The latter can be compared to specific map data for position estimation.
[112] describes magnetic field measurements for absolute localization (magnetic signatures and advanced map data), train integrity with magnetometer arrays at the train front end and rear end, as well as train odometry. A 2021 measurement campaign with the DB advanced train lab measurement vehicle is described.

4.1.6 Onboard sensors and systems

The section briefly lists the most important onboard sensors and systems with advantages and related challenges. The latter must be addressed with appropriate architectures (combination of sensors) and algorithms (sensor fusion). The LWG document [113] contains a similar effort that can be consulted as a complement.

4.1.6.1 GNSS receivers and antennas

Onboard GNSS must comprise antennas and receivers. The antenna position must be known with respect to an agreed vehicle coordinate frame. There can be several antennas and receivers. Receivers should be fit for signals from different satellite constellations (GPS, Galileo, etc.) and in different frequency bands (L1, L2, etc.). There can be correction information from SBAS (including EGNOS) and network sources. EGNOS can provide integrity information on the validity of a received satellite signal. In its basic form, a GNSS receiver internally processes pseudo-range and Doppler frequency shift measurements from each satellite in view. More advanced methods are required to

utilize the phase shift information in the satellite signals. Real time kinematic GNSS (RTK GNSS) employs the information of base stations to provide improved accuracy. For further background, the reader is referred to the GNSS handbook [72].
Advantages:

- Absolute position in 3D reference frames and speed information can be obtained without extra track infrastructure.
- GNSS is suitable for interoperability.
- GNSS can be used for tightly coupled and loosely coupled integration with other sensor data.
- Advanced GNSS (RTK, PPP, correction data, etc.) can be utilized for increased accuracy.
- In principle, a lot of information about the quality of the GNSS solution is available. In the simplest case, GNSS can be discarded if there are too few satellites available (for instance, when the vehicle enters a tunnel).

Challenges:

- GNSS requires satellite signal reception. However, there are many areas without sky view in the rail domain. There are many local disturbances (non-line-of-sight, multipath).
- The GNSS signals are submitted over the air. There is a risk of signal jamming and spoofing, where the latter requires much more effort by the antagonist.
- Advanced GNSS techniques can be complex.
- Rail-certified GNSS antennas are required. Sub-optimal antenna placement or mis-matched antennas (L1 only for a multi-frequency receiver) can lead to decreased performance.
- Reasonable rates are in the 1 … 5 Hz range for the position solution of a GNSS receiver. Due to the internal processing, there is a temporal correlation in the measurement error. This effect can often be seen in deteriorated performance while entering areas with difficult or no reception (for instance, upon entering a tunnel).
- GNSS receivers can provide accuracy information for the internally computed solutions. Depending on the receiver and receiver settings, these data can be too optimistic or over-confident. A requirement on reporting conservative accuracy information for rail-specific GNSS receivers can be derived for later certification.

4.1.6.2 Inertial measurement units

IMU contain accelerometers and gyroscopes that measure specific forces (acceleration and gravity) and turn rates in the sensor coordinate frame. Most IMU are realized in micro-electromechanical systems (MEMS) technology and available at low cost. The orientation and displacement of the sensor frame with respect to the vehicle frame must be known. The lateral IMU placement on the vehicle should be in the center. Background on IMU technology can be found in [75].
Advantages:

- IMU rates can easily be in the range of 100 Hz.
- Cost aspects. Several low-cost IMU can be installed to provide improved signals and redundancy.

Challenges:

- MEMS IMU exhibit slowly drifting bias errors that need to be estimated. IMU need to be calibrated with respect to the vehicle coordinate frame.
- Not all IMU measurements are due to vehicle motion. Vibrations from the vehicle or even passing vehicles can be seen.
- Standstill and motion detection can be performed on IMU data.

4.1.6.3 Velocity sensors

Several velocity sensors are common in the rail domain. Measurement principles include wheel rotation, radar, and optical approaches.
Advantages:

- The sensors provide velocity information (speed and driving direction, forward/backward).

- Standstill can be detected.
- The mentioned principles are common in the rail domain and commercial rail-certified sensors are available.

Challenges:

- Wheel rotation sensors are subject to slip and slide errors. Slip occurs on actuated wheels. Slide occurs during braking.
- The performance of radar and optical sensors can depend on the environment conditions (surface, weather, snow, etc.).

4.1.6.4 Balise readers

Balise-supported localization requires track-side infrastructure and information about the balise positions.

Advantages:

- Safety aspects are well-addressed in balises.
- Balises are part of ETCS already.

Challenges:

- Infrastructure costs for operators (installation, maintenance, monitoring).
- Difficult access for experimental development (need for balise positions, safety concerns with access).
- Balise information is only provided when passing a balise.

4.1.6.5 Communication systems

Localization using communication systems has great potential as complementary source of information. Especially the widespread introduction of FRMCS can yield information that might be used in similar way as GNSS signals. Communication technologies include ultra-wideband (UWB) with beacons on the infrastructure, 5G and FRMCS with the respective base stations, and SRC and T2T-communication (R2DATO WP48.4).

Advantages:

- Novel localization measurements become accessible in the rail domain. These include time-of-arrival, time-difference-of-arrival, angle-of-arrival measurements that are already explored in other domains. Measurement models for inclusion in sensor fusion algorithms are readily available [79].
- There are relations to GNSS signal processing in a receiver that can be utilized.
- Communication systems can be placed in tunnels.
- Relative localization via exchange of messages between vehicles can facilitate further use cases.

Challenges:

- UWB requires beacons in known locations.
- Safety aspects related to open communication standards need to be addressed.
- Limited availability of commercial and especially railway-specific hardware for the novel communication approaches.
- Interfaces to onboard localization hardware must be defined.
- SRC applies to short distances only.

4.1.6.6 Electromagnetic sensors and systems

The recent past has seen a number of approaches that sense electromagnetic environment. These include eddy current sensors, difference inductance sensors, magnetometers and magnetometer arrays. Magnetometer arrays are investigated in one demonstrator in R2DATO WP22. The sensor placement differs on the vehicle. The sensors record data at frequencies of 100 Hz and higher. Correlation of the recordings of two on-vehicle sensors heads spaced at a known distance yields

speed and direction information. From the warping of the signatures, the acceleration can be determined. Correlation of the signatures with previously recorded and georeferenced data (specialized maps) can be used for fingerprinting localization to obtain absolute position information. Several approaches are in a development stage but the TRL is still low.
Advantages:

- Velocity information via signature correlation is straightforward. Also, acceleration can be derived.
- With specialized maps, signature matching can provide absolute position information in GNSS-denied areas.

Challenges:

- Robustness and transferability to different vehicles needs to be shown. Calibration must be addressed.
- Electric motors and their power electronics can disturb the electromagnetic spectrum in all frequencies. Effects on the sensors need to be shown. This concerns the use on electrified vehicles as well as passing trains.
- The rail environment is full of large and moving ferromagnetic objects that have an effect on the sensor readings.
- Specialized map data with electromagnetic signatures is required for fingerprinting approaches. The effects of, for instance, track maintenance needs to be considered to see if maps are still valid.
- The computational demands need to be assessed as well as means for modular combination with other sensor data.

4.1.6.7 Cameras and lidar

Cameras and lidar are optical technologies that are widely used for perception, with future application in ATO. Lidar provide point clouds in the sensor coordinate frame. Cameras record images as unstructured information that is easily interpretable by a human but that needs to be algorithmically extracted by a machine. Earlier image processing worked on the extraction of engineered features. This may still be valuable in the rail domain, with the common structures seen by an on-board camera (tracks, switches, signals, sleepers). Optical flow can be related to vehicle velocities. The majority of current research uses machine learning / neural networks / deep learning to perform detection in the images. However, the dependency on training and the black-box nature with limited interpretability is obviously challenging.
Advantages:

- There may be access due to the use for perception without installing extra hardware.
- There is much research ongoing beyond the rail domain.
- The potential of recent deep learning advances can be used.
- Velocity information and landmark recognition can be realized.

Challenges:

- The limited understanding of deep learning systems, black-box nature with difficult-to-predict error characteristics.
- Cameras and data privacy.
- High data volumes, storage and processing performance concerns.
- Weather and lighting conditions, dirt on the sensor.

4.1.7 Sensor fusion algorithms

Here listed are general sensor fusion algorithms and their advantages and disadvantages for map-supported localization of rail vehicles.

4.1.7.1 Kalman filters

Kalman filters can be considered as “the workhorse of estimation” due to their widespread use since the 1960s. Although the KF theory has been designed for linear state space models, the first significant application was already a nonlinear navigation problem in the Apollo mission. It can be seen as the immediate development of the extended KF (EKF) in which linearization is performed over recent state estimates. A widespread misconception is that Gaussian noise is required. However, the original Kalman filter development did not specify the exact distribution but merely required known noise statistics (mean, covariance) for which an optimal estimator (in the minimum variance sense) was derived.
There are numerous nonlinear KF variants. Besides the aforementioned EKF (linearization based, analytical or numerical Jacobian matrices) the so-called sigma point filters are popular. Instead of linearization, deterministic sampling and weighted sample mean and covariance computation of the transformed sigma points is applied in the respective KF time and measurement updates. Sigma point KF include unscented KF (UKF) and cubature KF (CKF).
Rich KF sources are [79] and [80]. An in-depth treatment of sigma point KF is provided in [114, 115].
Advantages

- KF are simple to implement and modular (time updates, measurement updates).
- KF have a solid theoretical foundation with, e.g., convergence results for linear systems.
- Well-designed KF can be robust with respect to modeling errors and simplifications, unknown initial states, etc.
- KF work well for mild nonlinearities when the state densities are well-described by a mean value and a covariance matrix.
- KF embrace uncertainties via covariance matrices in all variables (states, measurements, process and measurement noise). That is, each KF state estimate comes with uncertainty information.
- KF combine physical modeling (state space models) with probability theory (noise distributions).
- KF are modular with respect to the included sensors. Adding extra measurements amounts to adding another measurement update (if the state vector allows prediction of that measurement).
- KF cope with varying sensor rates and outages. The KF works on an internal update rate that can be set independent from the sensor rates. That is, output is provided at that specific rate regardless of the available measurements.

Disadvantages

- The involved densities (noise and state densities) must be well-represented by a mean value and a covariance matrix. An example where this is not the case is the position uncertainty of a train after passing a switch. Here, a bimodal density is required to model each path hypothesis.
- Tight integration of map data is difficult if the path in the network is not known (this is the case for onboard localization without route information).
- The inherent KF robustness can mask errors, especially with numerous sensor sources. Care must be taken by testing the effect of each respective measurement update. In that sense, fewer sensors and loosely coupled GNSS integration (receiver-provided positions and speeds) can be easier to understand and monitor than tightly coupled GNSS integration (pseudo-ranges, Doppler, phase).

4.1.7.2 Particle filters

Particle filters (PF) approximate the Bayesian filtering density with a large number of weighted samples. The particles are propagated in each time step so as to randomly cover the relevant areas of the state space. There are issues with high-dimensional state space models that are related to the curse of dimensionality (difficulty to draw meaningful samples that represent the posterior densities well). Furthermore, the PF results are random in the sense that two repeated runs on the

same data yield results that differ numerically. While this can be dealt with, it is perhaps more difficult to accept with regard to strict testing. There are advanced PF variants (marginalized or Rao-Blackwellized PF) that combine PF and KF for the nonlinear and (almost) linear state components in a state space model.
Rich sources for PF are [79] and [80].
Advantages

- PF have been invented for severe nonlinear problems and can deal with multi-modal state densities. Their application to especially challenging problem beyond the KF is common, including fingerprinting of electromagnetic signatures.
- PF are simple to implement in basic forms.
- PF provide advanced uncertainty information (particle solution to the Bayesian filtering problem).

Disadvantages

- PF have issues in high-dimensional state space models. More than 2-3 states require extra measures that are no longer simple. There can be PF degeneracy in the sense of only few particles with non-zero weights after the PF measurement update. Here, the particle approximation no longer represents the true state posterior density well.
- There is always randomness in the PF results due to the inherent random sampling in the state propagation.
- An increase in the number of particles improves the approximation at increased computational costs. Due to the resampling step in the PF measurement update, the computations cannot be fully parallelized.

4.1.7.3 Moving horizon estimation

Moving horizon estimation (MHE) [116] is an optimization approach to filtering in state space models. Similar to the dual problem of model predictive control, the states are estimated by optimization of a cost function over a number of recent time steps. While there are relations to KF (which is also rooted in the iterative optimization of a cost function for a model) the execution is much different.
Advantages

- The optimization viewpoint can be made robust to many error sources.
- A range of (numerical) optimization approaches can be used.
- If the optimization problem can be shown to follow a certain structure (convex) theoretical results apply in the sense of convergence and optimality results.

Disadvantages

- MHE requires storing the data over a time horizon.
- Extra steps are required to obtain uncertainty information.
- Numerical optimization is required over several decision variables. Convergence needs to be shown.
- MHE can exhibit higher computational complexity depending on the problem at hand.

4.1.7.4 Kalman filter banks

Kalman filter banks here subsume all approaches that employ several Kalman filters in parallel. The knowledge that vehicles travel along tracks sequences in the railway network motivates the idea of several paths and associated on-path Kalman filters. The on-path KF inherit the positive KF properties listed above. Map integration and the path concept are explained in [105]. The correct hypothesis must be determined by using the KF residuals (or related quantities that can be derived from the respective on-path KF). If the KF or hypothesis performance is assessed over a number of recent time steps, there is a nice relation to the MHE above. Whereas PF approaches randomly populate the track network, explicitly addressing all paths underneath the vehicle in a KF bank provides a “minimum number of hypotheses / particles”.
Advantages:

- KF banks can be used to divide localization into a path estimation and an on-path localization problem. Advantages from PF, KF, and MHE can be combined.
- No randomness as in PF.
- Represent the multi-modal position uncertainty well in contrast to KF.
- KF banks are modular with respect to the employed sensors.

Challenges:

- Computational complexity between KF and PF.
- Implementation more complex than KF.

4.1.8 Conclusions and recommendations

From the study on localization systems follow a number of conclusions and recommendations.

- Localization is of key importance for VCTS in the operational, tactical, and strategic layers.
- Localization should be realized as separate onboard component with access to sensor and map data. This is in accordance with the OCORA LOC-OB component and the ASTP (with access to a digital register DR) topic in R2DATO.
- There are many ongoing developments in terms of new sensors and measurement principles, access to map data, and algorithms. It is important to prepare their flexible inclusion in future systems, so as to not miss out on their potential. Of course, this can be a challenge in the development of standardized architectures and approaches.
- Important literature has been summarized. Yet, any such list is bound to be incomplete and over-simplifying.
- Onboard sensors and systems shall include GNSS, IMU, velocity sensors. The incorporation of generic position sensors can unify balise approaches and more innovative fingerprinting positioning solutions. Communication systems have the potential to be used in a way similar to GNSS.
- A very brief algorithmic perspective shows Kalman filter bank approaches as viable combination that inherits favorable KF, PF, and MHE properties.
- Finally, advanced concepts are difficult to fully assess based on literature studies only. Data and software are needed to compare approaches. Respective coding and data gathering activities should be increased.

4.2 VCTS VEHICLE INTERFACE AND COMPONENT INTERFACES CONCEPT WITH DATA STREAM ANALYSIS

Chapter 2 presented the principal functionality of VCTS, which was developed in previous Shift2Rail projects, including X2Rail-1/3/5, MOVINGRAIL, and others. This chapter builds upon these concepts by proposing components and their interfaces. Furthermore, a preliminary data stream analysis between these systems, components, or their interfaces is presented.

4.2.1 Vehicle communication architecture and interfaces

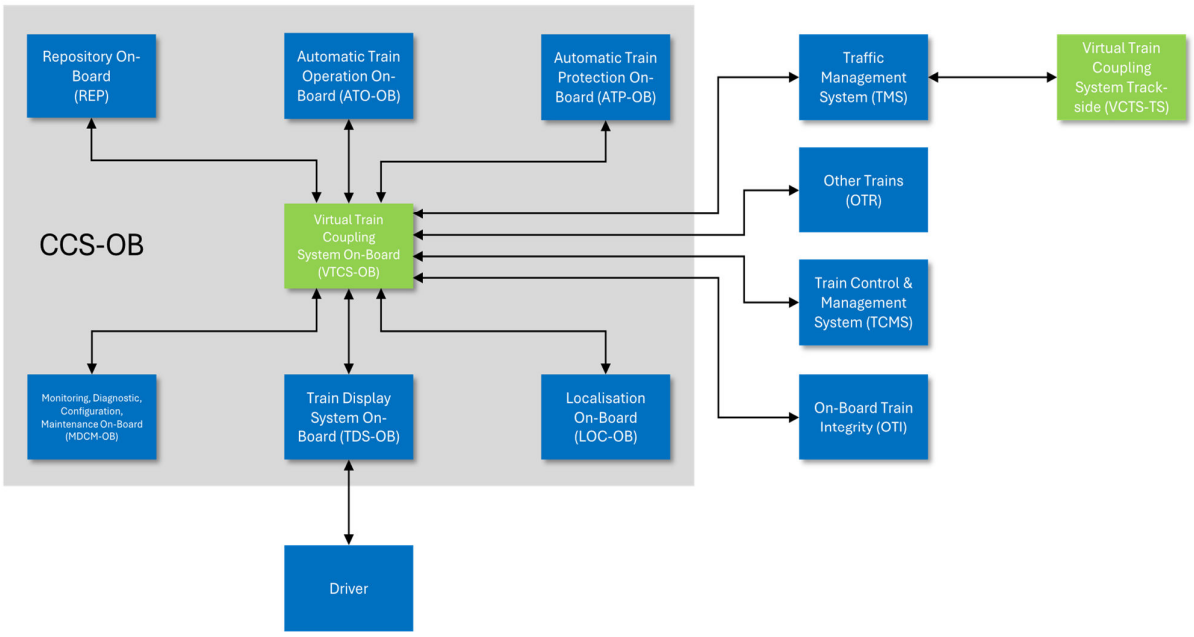

Figure 29: VCTS-OB interfaces

Figure 29 presents an architectural view of the VCTS on-board systems and their interfaces to other on-board and trackside systems. The centre of the picture depicts the abstracted VCTS on-board system, which provides an overview of the technical environment and the systems involved or needed for VCTS operations. VCTS is part of the onboard Command, Control and Signaling system (CCS-OB). The known or designed functional interfaces are marked.

One step closer, the VCTS system is a distributed system over several trains into a convoy. It consists of a functional tactical layer and an operational layer at every train head. Between all system parts, a transparent communication at application level is assumed. This is enabled by an intra train communication system, a T2G (FRMCS) and a T2T communication system. Because both train heads have a T2G gateway, this communication could be redundant within one train. It is also be used for communication between trains via infrastructure. When trains traveling in smaller distances on a line, than a direct T2T link provide advantageous characteristics like reduced latency and increased reliability.

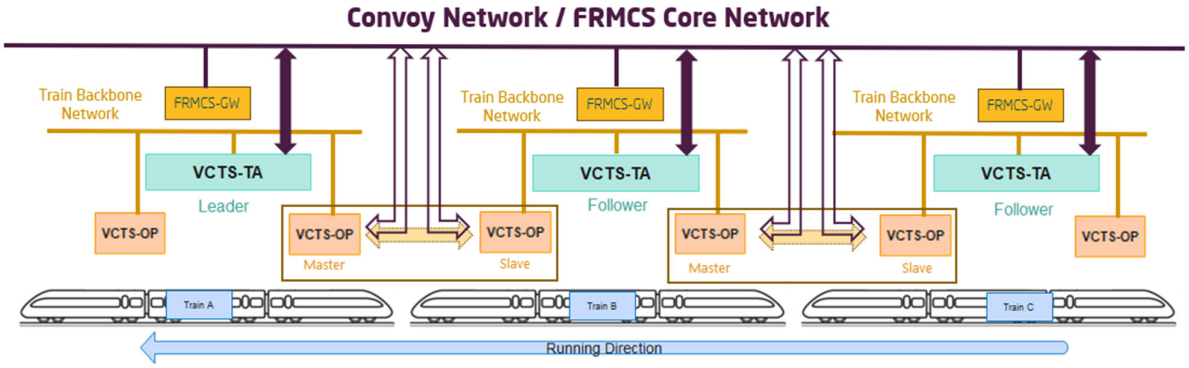

Figure 30: Technical convoy communication structure with FRMCS. Source: Indra Sistemas S.A

At the time of writing this report, the SP had not published any specifications about the new vehicle communication structure. It should be noted that new developments in the context of CONNECTA, Safe4Rail, X2Rail, OCORA, and RCA are known, but have a preliminary character. In order to prevent speculation regarding future System Pillar specifications and TCN standardisations, it is essential to base the following analysis on the actual standardized Train Communication Network (TCN) of IEC 61375. A migration to the System Pillar proposed Next Generation TCN (NG-TCN) at a later time is possible by adapting the conventional communication systems to the new proposed communication and computation architecture/structure. As a first design step or analysis step, the general communication structure of the vehicle and the communication partners of the VCTS system must be defined.

The fundamental communication structure of a Train Communication Network (TCN) in accordance with IEC 61375 is based on a dynamic Ethernet Train Backbone network (ETB) with Train Backbone Nodes (TBN) functioning as routers between the ETB and static Ethernet Consist Networks (ECN). There are various technical implementations of the Ethernet-based TCN, which are beyond the scope of this discussion for the sake of simplicity.

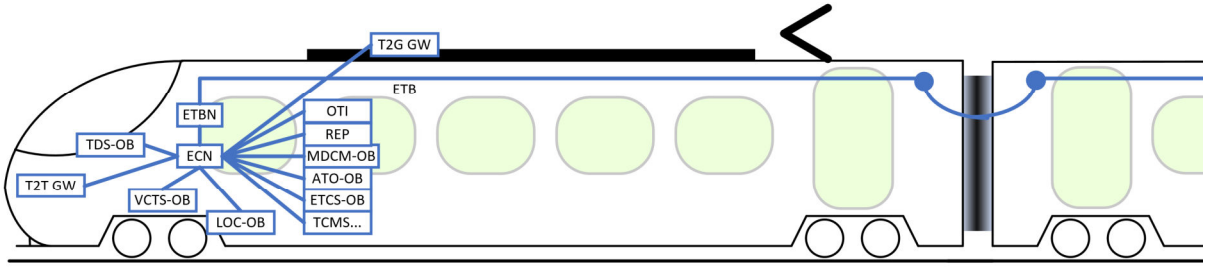

Figure 31: TCN architecture

Figure 31 illustrates the general structure of an Ethernet-based TCN network. All TCMS components must be connected to that network. The components of VCTS and its supporting environment, as depicted in Figure 31, must be connected to the proposed TCN network in a meaningful manner. The following assumptions are made:

- The VCTS-OB is computed on a separate ECU and connected to the ECN network of a train head. Each train head has a VCTS-OB. The front head is equipped with the leading VCTS-OB system, while the rear head is equipped with a slave VCTS-OB system for checks and communication with trains behind.
- The ETCS-OB is abstracted to a black box for simplicity, which is also connected to the ECN network.
- The ATO-OB is a concentrated system with a connection to an ECN network.

- On each train head exists a Localization System (LOC-OB). Please refer to T48.4. This combines absolute localisation on the track and relative localisation between trains of the VCTS convoy. Technically, it establishes a train-to-train communication for VCTS too, which is functional separated. The main ECU of LOC-OB and T2T-COM/OTR is connected to the ECN consist network of the train head.
- It is assumed, that the VCTS T2T communication occurs between two VCTS application-level gateways. Each train head is equipped with a gateway of this type. The gateway is connected as an ECN node to the consist network of the train head. The VCTS data stream is transformed at the application level from the ECN message format to a T2T format and vice versa. The gateway is responsible for ensuring the safe, timely and secure transmission of data to the connected gateway. It should be noted that there is no direct communication between the TCN networks of both trains.
- The TMS is located on the trackside and communicates via T2G communication with the VCTS-OB. The TMS integrates the VCTS Strategic Layer (SL).
- It is assumed that all other TCMS systems, monitoring devices/systems (MDCM-OB), and the train integrity system (OTI) are available from the consist network of the train head.
- The Train Display System (TDS-OB) is assumed to be a single device connected to the ECN network of the train head.
- It is a mainline passenger railways application (refer to Chapter 3.2.1) is assumed.

On the basis of these assumptions, all systems with a relation to VCTS are materialised as a component and connected to the vehicle communication system. This constitutes the basis for the subsequent data stream analysis.

4.2.2 Data stream analysis

In order to analyse the network usage of the designed VCTS functionality and the proposed devices, a preliminary data stream analysis is conducted. This provides an initial estimation of the expected network usage between different systems of/for VCTS and over different communication vectors.

The VCTS functionality is modelled using a Capella MBSE model, in which the involved systems as communication partners and their functional exchanged information are defined. This information is used to summarise the communication behaviour of communication devices and the usage of the networks or communication paths.

The operational scenarios of the VCTS (see X2Rail-3 D6.1, chapter 9) exhibit markedly disparate communication behaviours, requirements and conditions. Consequently, each scenario is analysed separately. A more detailed description of the VCTS functionality and communication behaviour can be found in X2Rail-3 Deliverable D6.2, chapter 7.3.

It is beneficial to distinguish between event-based communication (message data) and periodic, repeated communication (process data).

In event-based communication, the majority of exchanged messages are relatively small and have a minimal impact on bandwidth. The primary concern is ensuring timely transmission and prevention of message loss. This aligns with the latency properties of the communication system and most messages use an acknowledgement reply message.

Periodic exchanged messages transmit status or state signals at a specified update rate. The bandwidth impact is limited due to the small message size and lower update rates. In general, the communication effort of operational technology systems (OT) is relatively modest in comparison to other IT applications. Modern wired Ethernet-based communication systems for railway vehicles provide a sufficient bandwidth. However, T2G and T2T communication have limitations in bandwith and latency.

The three main phases of a VCTS session are used as the three scenarios for analysis. These are:

- VCTS coupling phase (Phase 1)
- Driving under VCTS supervision (Phase 2)
- Termination of the VCTS session (Phase 3)
-

For the purpose of the data stream analysis, it is assumed that a set of three trains are running on the same line. All trains establish a VCTS session, travel in a VCTS convoy and terminate the VCTS session at the end. As a reasonable example, the expected data streams of the leading train are analyzed.
The first analysis is a comparison of the amount of event-based and periodic messages in the three main phases.

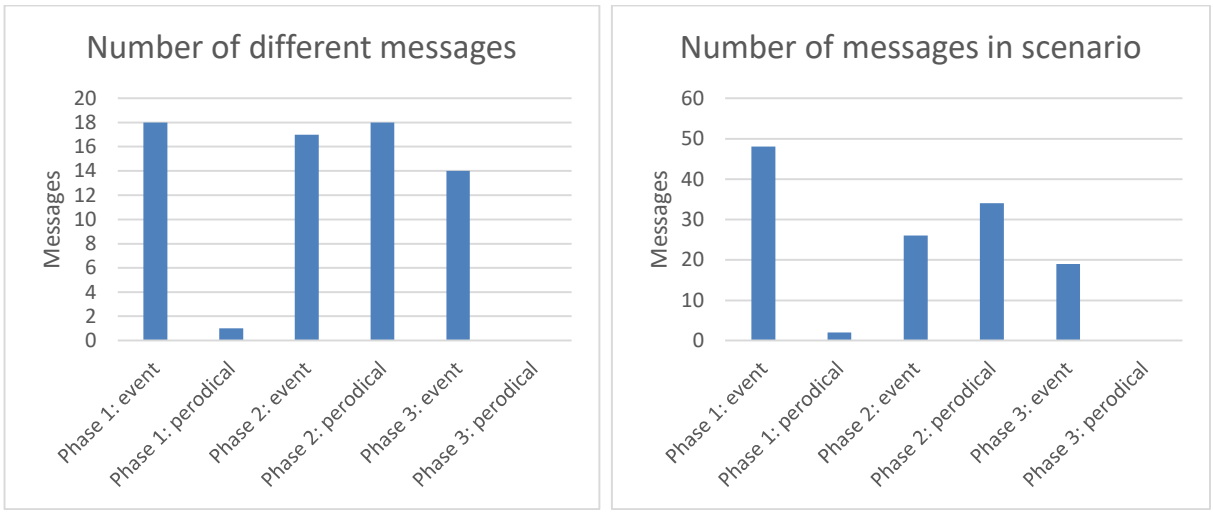

Figure 32: Count of different messages (left) and the overall count of messages (right)

Figure 32 illustrates the number of distinct event-based and periodic messages, classified according to the three phases. The number of distinct messages serves as a general indicator of the bandwidth utilisation and the intensity/diversity of the communication. It should be noted that the message types may be utilised on multiple occasions. Figure 3 illustrates the minimal number of messages required for each phase. The periodic messages are repeated in cycles.

Figure 32 demonstrates that in the coupling and termination phase, event-based messages are the dominant form of communication. In the context of an established VCTS convoy and driving under VCTS supervision, the majority of exchanged messages are periodic.

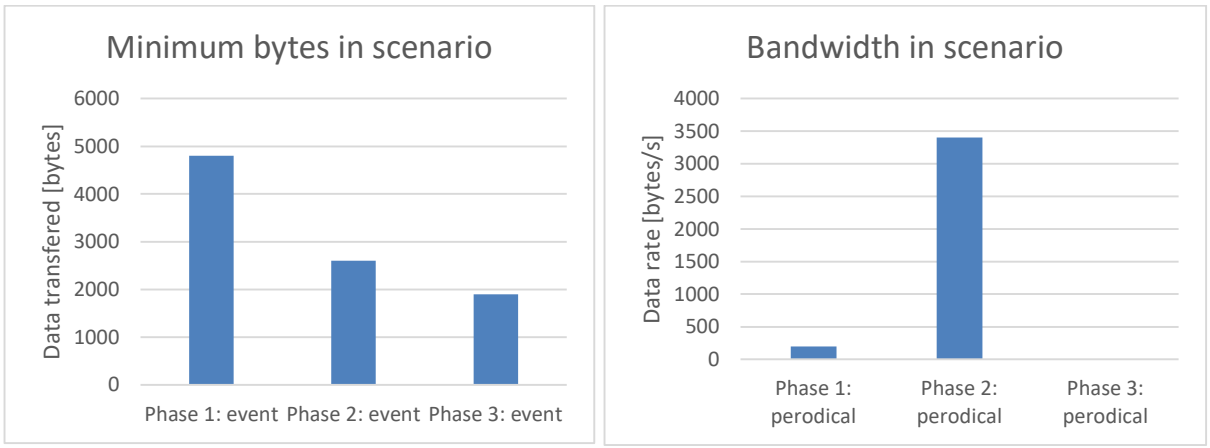

Figure 33: Minimum necessary bytes for event-based comm. (left) and bandwidth usage for periodical communication (right)

Figure 33 (left) shows the minimum number of bytes required for event-based messages, assuming a mean message length of 100 bytes. Figure 33 (right) depicts the bandwidth usage of periodical repeated messages with an assumed frequency of 10 Hz, expressed in bytes per second.

A second analysis focuses on the communication path and the usage of communication systems. All devices are connected to the ECN network of the vehicle, which serves as their main communication interface. (Close to) all traffic will pass the ECN network of the train head. The majority of the VCTS-OB traffic is transferred for redundancy by the train-wide ETB to the second VCTS-OB, which is located on the opposite train head. Traffic destined for the trackside is passed through the Train-to-Infrastructure Gateway. Direct communication between trains is transferred by the Train-to-Train gateway.

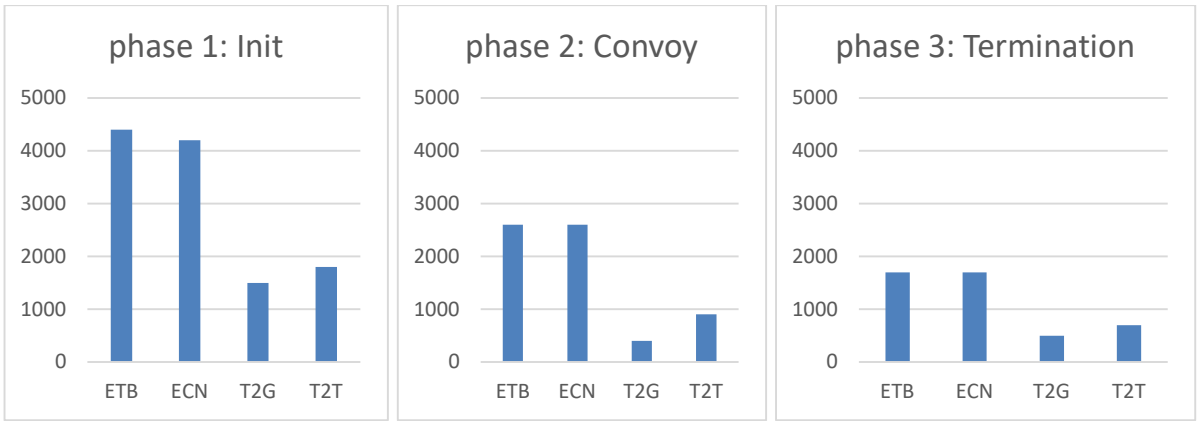

Figure 34: Transferred data [bytes] for event-based communication for each phase and route [bytes/phase]

It is assumed, that all three phases are conducted with a minimum of communication effort. Figure 34 displays the transferred data for the main communication pathways. During the inaugural phase 1, the exchange of status and control messages to initiate a VCTS session needs the most bandwidth, with over 40 messages being exchanged. However, only a subset of these messages is required during the third phase to terminate the VCTS convoy. In the main phase 2, a relatively smaller proportion of communication effort is dedicated to event-based messages.

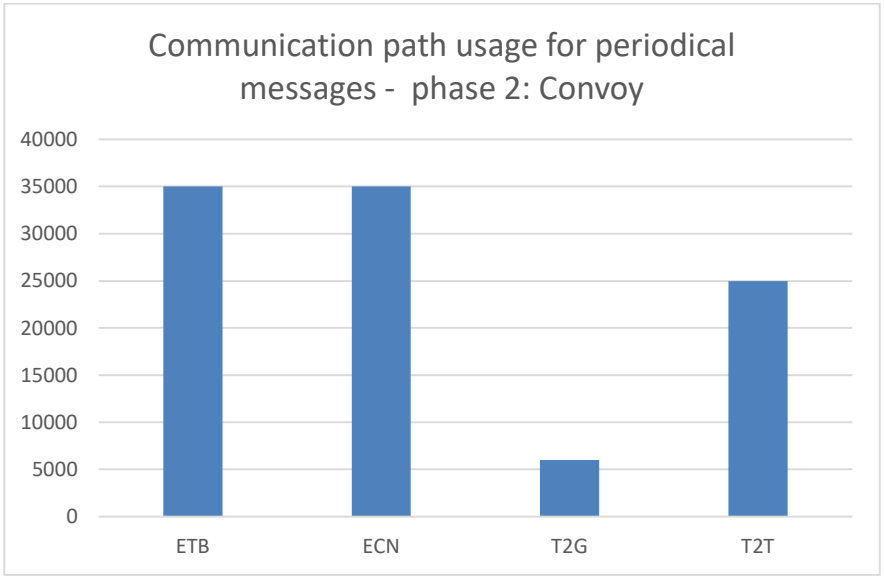

Figure 35: Data rate of periodic data transmission for the main communication paths [bytes/s]

The expected data rate of periodic data within a VCTS convoy is much higher than the event-based communications. Figure 35 shows the bandwidth utilisation for the main communication pathways. The VCTS data traffic traversing the wired networks ETB and ECN exhibits the highest data flow, as the majority of the data is routed through these networks. However, it is relatively modest in comparison to the maximum transmission capacity. The T2G path is utilised by just 4 periodic messages. . The recently introduced T2T communication is used by the VCTS system for a significant portion of its bandwidth. Alternatively, the T2T traffic between the trains could be rerouted via the T2G gateways.

4.3 TCN APPLICATION PROFILE CONCEPT

Based on the overall system design in chapter 5.1, who describes the tactical layer and its behaviour in general, this section begins with a more concrete application of the communication behaviour to the standardized train communication networks according to IEC 61375. This is a good basis for further structuring the VCTS communication and integrating it into a potential train network. The structures described in the TCN standard part IEC 61375-2-3 on the communication profile and part IEC 61375-2-4 on the application profile should be applied conceptually to the VCTS system. However, the methods presented in the NG-TCN should already be considered in the background (CTA-1 D4.3; CTA-3 D5.1).

The following structure is based on the IEC 61375-2-4 standard. Chapter 4, of this standard, describes the design pattern of distributed train applications with ‘function leader’ and ‘function follower’. However, the VCTS system is not a TCMS system, which means a continuous function chain from an operator action to reactions on systems (distributed across the train) such as the brake. But the basic principle can be adopted. There will be external commands or operator actions that act on a ‘function leader’, who integrates the core functionality and decision making. The ‘function leader’ controls distributed ‘function followers’. These maintain the connection to other systems and return statuses and requests to the function leader as local representatives. The functional connection between the elements considered here is direct, although it should be noted that the technical implementation may involve the use of several physical communication systems. For example, communication to and between the function followers takes place via the train-internal networks and via train-to-infrastructure or train-to-train interface.

4.3.1 VCTS communication architecture

Figure 36 displays the general communication architecture used for VCTS. All trains have a continuous wireless connection to an infrastructure-based FRMCS core network. All other infrastructure services, other trains and the strategic layer are reachable by this network. The drawback of an FRMCS T2G interface could be uncertain or extended message transport time delays. When trains are closer between each other, they could use a direct link of a train-to-train communication.

The tactical layer is relaying to the FRMCS core network only, because it needs to communicate to all trains of the convoy in parallel.

The operational layer could use the FRMCS network when the trains are far from each other and the T2T link is not established. If this link is usable, especially when the trains are closer together, than the private and low latency link of the T2T communication is used.

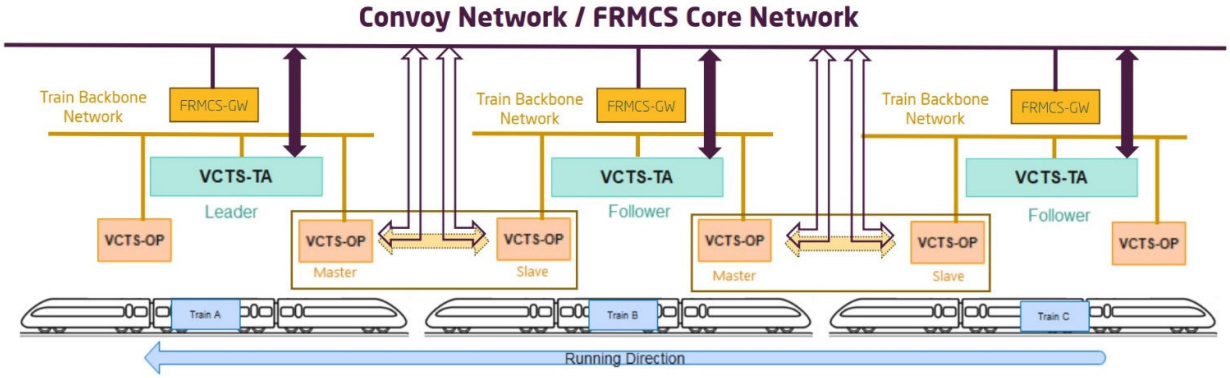

Figure 36: Functional communication architecture

4.3.2 Application functional breakdown structure

The basic functional architecture of VCTS consists of four layers (Figure 11), the Service Layer, Strategic Layer, Tactical Layer and Operational Layer. Only the Tactical Layer and the Operational Layer are considered in this section.

According to chapter 5.1, the strategic layer is responsible for determining the composition of an impending VCTS convoy, as well as the selection of the train designated to assume the role of the tactical layer function leader (VCTS Tactic FL). Each train head is equipped with a ‘function follower’ (VCTS Tactic FF), which functions as a permanent interface and distributes the status and commands of the tactical layer to all vehicles within the VCTS convoy. The ‘function leader’ in the VCTS convoy can also change instance and position, whereby the ‘function followers’ are permanently present on each train head. The function leader of the tactical layer maintains a functional connection to the VCTS strategic layer.

As also outlined in chapter 5.1 each train in the VCTS convoy is equipped with its own VCTS operational layer. Within a convoy, all operational layers of the trains are connected by a master-slave structure, wherein the leading trains rear head plays the master role und the following trains leading head functions as its slave. This configuration is repeated for all train gaps within the convoy. Because of this structure, the leading train demands the operational behaviour of the following train.

As a consequence, and following the function leader/follower pattern of IEC 61375-2-4 standard, the operational layer slave role of a following train must be the function leader of the VCTS operational layer (VCTS-OP FL) in this train. It gets the directives from the train ahead and transforms it to commands/controls for train-local systems. The behaviour of the following train is controlled by the function follower or master role at the rear train head (VCTS-OP FF).

The first train in the VCTS convoy has no train ahead to follow, but it gets its objectives from the train-local tactical layer function follower.

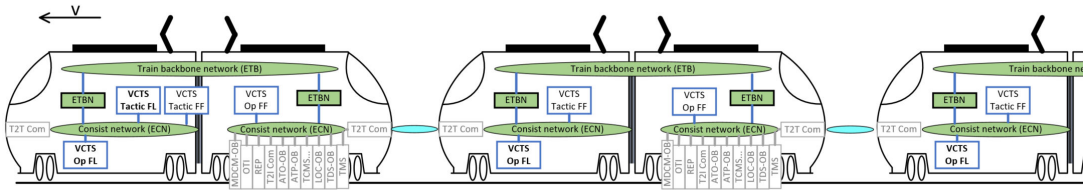

Figure 37: Functional distribution of Tactical and Operational Layer over VCTS Convoy (FL – function leader, FF – function follower)

Figure 37 shows the distribution of the functional elements of the tactical layer and operational layer across a VCTS convoy. For simplicity, only the two train heads of a train are shown. The Ethernet networks within the trains are shown in green. There is a T2T data connection between the trains.

It is assumed that the messages of the VCTS system (within trains) are transmitted via TRDP messages. The application-specific messages are clearly structured in accordance with IEC 61375-2-4 Chapter 5.2.1 and the structure can also be applied to the VTCS system.

From the ‘System Analysis’ of the MBSE Capella model, the function groups, which are referred to as missions, can already be recognized. The VCTS ‘FunctionId's’ and sub-functions can be derived from this.

The ‘ChannelIsd’ can be adopted unchanged.

The definition of the sequence numbers according to IEC 61375-2-4 chapter 5.2.9 [117] can also be adopted. The trains within a VCTS convoy are also numbered.

5 MODELLING THE OPERATIONAL CONCEPT (TACTICAL LAYER)

5.1 VCTS MODELS

5.1.1.1 Introduction to tactical layer

According to X2Rail-3 [4], and following the architecture of Figure 11, the tactical layer is located between the operational and strategic layers. The strategic layer decides the objectives to be met (what), the tactical layer decides how to carry them out (how) and the operation layer executes the directives (execution). Strategic layer: it decides which strategy to follow to achieve defined objectives and plan. Tactic layer: it decides which actions to take to comply with the strategy. Different tactics are generated, and it is decided what to execute based on the objectives established in the strategic layer. It translates high-level strategic objectives into actionable decisions that influence the real-time performance of train movements. The tactical layer oversees coordinates the movement of the consists that make up the platoon from the moment the incorporation request is received until the platoon is dissolved. Operational layer: it executes the movement directives it receives from the tactical layer and always guarantees safety, that is, that the distance between the trains is safe.

Information flow between layers is descending (Strategic layer > Tactical layer > Operational layer), ascending (Operational Layer > Tactical Layer > Strategic Layer) and bilateral (from left to right and from right to left between train consist).

- Descending: the strategic layer sets strategic objectives to meet the planning. This layer reports this to the tactical layer, which generates movement directives based on different tactics and communicates this to the operation layer. The operation layer receives the directives and executes them as long as it is safety.

- Ascending: the operational layer informs the tactical layer of the actions being executed. Based on this, the tactical layer will vary or not the movement directives generated, to always adjust to the strategic objectives. The tactical layer informs the strategic layer of the results of the actions being executed, so that this layer can modify, if necessary, the strategy to be followed to achieve the planning, or even modify the planning itself.

- Bilateral horizontal information flow: in the operational layer, the local layer, the trains must exchange information between them to carry out the movement directives safely. In turn, in the tactical layer there must also be a horizontal flow of information at platoon level, to transmit the information of the tactics to follow and the movement directives to each train that makes it up respectively.

5.1.1.2 Objectives and Characteristics of the tactical layer

The objective of the tactical layer is to generate movement directives based on tactics to meet strategic objectives. Therefore, it is important that this layer is able to interpret the information it receives both horizontally from the platoon and vertically (from the strategic layer and the operational layer) to act accordingly. It is not the objective of the tactical layer (or the strategic layer) to assume functions that have to do with safety. Safety resides in the operational layer, although the tactical layer defines movement directive considering safety rules.

The tactical layer has the following main characteristics:

- It is the link between the operational and strategic layers.
- It exchanges information with the strategic layer: it needs to know what objectives to accomplish (what to do) to define movement directives (decide how to carry them out).
- It exchanges information with the operational layer: to transmit the actions to be executed and their status.
- It has contextual information: it obtains information from the entire platoon and the rest of the systems.
- Real-time decision: linked to the previous characteristics and due to them, the tactical layer can receive real-time data from both the operational layer and the strategic layer, process it and generate movement directives based on the reported conditions and objectives.
- Adaptable and dynamic: the tactical layer adapts quickly to short-term changes, such as delays or system interruptions.

5.1.1.3 Relationship of the tactical layer with the operational and strategic layer

As previously mentioned, the tactical layer operates at an intermediate level between the operational and strategic layers. In this way, the tactical layer ensure that strategic objectives are met by aligning with real-time train operations. In the VCTS system the operational layer is responsible for execute movement directives distributing them along the train consists. It must ensure that the movement directives established by the tactical layer are executed safely, especially those related to the joining or leaving of the platoon.
The detailed information flow and decision-making processes between these layers are as follows:

- Descending - Strategic Layer >Tactical Layer > Operational Layer:
    - Strategic layer to tactical layer: the strategic layer provides high-level objectives, the strategy that the system should follow. These guidelines shape the decisions that the tactical layer makes.
    - Tactical layer to operational layer: the tactical layer provides real-time movement directives to the operational layer (e.g. specific train movements, speed adjustments).
- Ascending - Operational Layer > Tactical Layer > Strategic Layer:
    - Operational layer to tactical layer: the operational layer informs the tactical layer of the action being executed at any given moment and provides to this layer the information required in each case (position, speed or anomaly data flows upwards). The tactical layer with this information reviews whether it needs to change or adjust the movement directives to meet the strategic objectives.
    - Tactical layer to strategic layer: the tactical layer informs the strategic layer of the results of the actions that are being executed at any given time. In this way, the strategic layer reviews and analyses whether it is necessary to adjust the strategy to comply with the planning. Or, if necessary, it reports non-compliance with the planning, therefore, the strategic layer should have to take some actions.

- Bilateral horizontal information flow: in the tactical layer, all the train consist of the platoon communicate horizontally, which is why it is important that there is a flow of information (movement directives). In turn, in the operational layer there must also be horizontal information flow, the neighbouring trains must exchange information to carry out the movement directives in a safe, stable and consistent manner.

For example, if a line is observed to be very congested, the strategic layer defines the strategy for coupling trains to relieve congestion on the line and comply with the timetable. The tactical layer receives this objective from the upper layer and decides that train A must couple with train B at PK X at a certain time. In turn, it is decided that the capacity maximization tactic will always be followed, so the minimum distance between the coupled trains will always be sought, if it is safety.
The tactical layer generates movement directives and informs the operation layer. The operation layer executes the coupling directives and ensures that can be executed from a safety point of view. In turn, the operational layer informs the tactical layer of the execution or not of the movement directives. If, for example, the coupling has not been possible, the operational layer informs the tactical layer, which sees if it can generate new movement directives to couple the trains in another area and thus adjust to the strategic objectives. In the same way, the tactical layer informs the strategic layer of the results of the actions that have been executed, to modify the strategy and even the planning if necessary. Following the same example, if it is not possible to change the directives to couple the trains, the tactical layer informs the strategic layer that the coupling has not taken place and therefore the planning must be changed, since the line will be congested and there will be delays.

5.1.1.4 Tactic Concept

A strategy establishes the overall vision, defining the long-term objectives and the general path to follow, that is, it is the plan that is followed to achieve one or several objectives. On the other hand, a tactic is the set of specific methods and actions that are used to achieve an objective (within a broader strategy). Tactics focus on concrete execution and adaptation to changing circumstances. ´

The strategic layer defines the objectives: the timetable, the coupling-uncoupling plans and the operational rules, that defines the approach on how to execute the coupling and uncoupling plans (energy saving, maximum capacity-minimum distance).

For instance, in the strategic layer, objectives are defined (to meet the schedule), to carry it out a strategic plan is generated (to couple trains A and B) and day by day, depending on the real situation, this plan (real timetable plan - RTTP) can be modified to meet the objective. The tactical layer already knows that the strategy is to couple trains, it decides how to do it, that is, it generates movement directives to couple planned trains. To couple Train A with Train B there are different ways to do it, and these must fulfil with the operational rules. It can be decided to do the coupling as quickly as possible, do the coupling keeping the minimum distance, look for the coupling looking for comfort, etc, but this is decided by the strategic layer.

The tactical layer defines the movement directives, based on all the above, which the operational layer executes. For example, from the point of view of the railway operator, the objective is to meet a timetable, but in each case an operational rule to follow is defined. Operator A decides that he wants to attract customers, so the tactic is based on always arriving first (optimize coupling and uncoupling to reach maximum speed). On the other hand, operator B seeks to be more sustainable, so its tactic is to reduce the carbon footprint by meeting the schedule (energy saving). At the same

time the infrastructure manager can save an operational rule to save maximum capacity setting minimum distance. The tactical layer while must follow the predefine operational rules, based on prioritization.

Tactical layer roles

To carry out the tactic (the collection of movement directives to fulfil with the strategic objectives), each of the different involved train consist must be aligned; It is necessary to define a leader, which lead the tactic and the followers, which collaborate with the leader to carry out the tactic. Note that the leader will be decided originally by the strategic layer, nevertheless this can be changed based on the tactic to be apply.

For instance, the strategic layer determines that the trains A, B and C, that have common destination (station Y), must couple to optimize the line capacity (selecting Train A as leader). And define that Train A will arrive on station Y at 14:00 on track 1, Train B will arrive on station Y at 14:07 on track 2 and Train C will arrive on station Y at 14:20 on track 3, establishing the uncoupling manoeuvre zone around 20-35km before the first switch of the station Y.

Train	Destination	Arrival time from destination
Train A	Station Y. Track 1	14:00 h
Train B	Station Y. Track 2	14:07 h
Train C	Station Y. Track 3	14:20 h

Table 3: Use Case – 1. Train B schedule.

To follow the detailed strategy, the tactical layer defines several roles along the route. Initially, when the trains are coupled forming the platoon, setting Train A as leader (the one in the head), and Trains B and C as followers (Figure 38). Train A - the leader - generates movement directives to fulfil the strategy. First, it informs the followers that they must stay coupled at a minimum distance (movement directive). The operation layer will execute the movement directives.

Figure 38: Leader-Follower role example (part 1). Source: Indra Sistemas S.A

When the platoon is reaching the uncoupling zone, 37 km before reach station Y, the leader in the tactical layer, to comply with the strategy, communicates with the follower Train B and then passes the leadership to it, so that the new leader is Train B and Train A becomes follower (Figure 39). This is because to comply with the strategy of Train A entering track 1 and Train B entering track 2, Train A must separate from the platoon, so it cannot continue being the leader. To do this, the tactical layer generates new movement directives, based on the existing traffic and the movement authorities of Train A, it is decided to carry out the uncoupling manoeuvre at 32 km before station Y. Increasing the distance between Train A and Train B to be able to be uncoupling and keeping Train B and Train C coupled. The leader communicates these directives to the followers and the operational layer executes them, that is, Train B decelerates to increase the distance to Train A and Train C does the same as Train B to maintain a safety coupling. The slave of Train B increases the distance between the master of Train A until they separate, and the rest of the consists maintain the safety distance based on relative braking distance throughout the entire platoon.

When Train A uncouples from Train B, the tactical layer informs the strategic layer that Train A is uncoupled and Train B is still coupling with Train C. It must be ensured that train A is switched to track 1, ensuring that the distances and times required by the existing safety system are met. Now the platoon consists of Train B and C only (Figure 40).

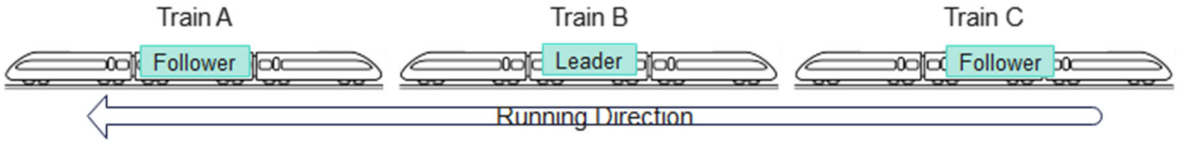

Figure 39: Leader-Follower role example (part 2). Source: Indra Sistemas S.A

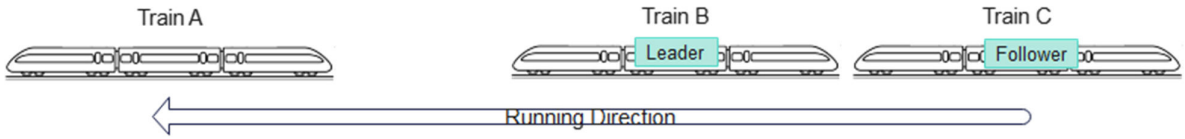

Figure 40: Leader-Follower role example (part 3). Source: Indra Sistemas S.A

To continue meeting the objectives (Train B must enter on track 2 and Train C on track 3), the tactical layer must generate new movement directives, still in the uncoupling zone. Based on the existing traffic and the movement authorities of Train B, it is defined to make the uncoupling at 25 km before station Y. Therefore, the leader, Train B, informs the followers of the new directive, to increase the distance between Train B and Train C. In this case, Train B remains the leader after communicating with Train C and reaching this consensus. The operational layers execute the directives, Train C decelerates and increases the distance with respect to Train B. Train C successfully uncoupling from Train B and the platoon is dissolved. The tactical layer informs the strategic layer of the uncoupling and the strategic layer checks whether the set objectives are met. It must be ensured that Train A is switched to track 1, Train B to track 2 and Train C to track 3, ensuring that the distances and times required by the existing security system are met. When the strategic layer sees that Train A, B and C are correctly uncoupled, the tactic is concluded, therefore each train will acquire its own leader role for its own train consist.

According to X2Rail-3 [4] definition, the operational layer executes movement directives involving at least two train consists. Furthermore, as previously mentioned, it must ensure safety (ensure that the distance between train consists complies with safety standards based on relative braking distance). To achieve this, it is also necessary to define certain roles in this layer: the master and slave roles.
In the operational layer, directives involving changes in the relative distance between two consists are generated during the coupling and uncoupling manoeuvres, and in the coupling mode itself (maintaining the coupling). Therefore, the roles of the operational layer can be simplified to master and slave. The master is the head of the train consists and the slave follows, and so on for the remaining consists. So, to successfully understand the entire operation, it is also necessary to define the operational roles

Operational layer roles

As seen before, local and operational roles of master and slave are defined in this layer. In the tactical layer, the leader role can be acquired by anyone and the follower as well as has been detailed, but the master and slave roles cannot. The master is the one who precedes following the direction. That is; by defining the direction of movement of the composition, the head and tail of each train automatically acquire their role.

For instance, continuing with the previous example, where the strategic layer determines that trains A, B, and C, with a common destination (station Y), must be coupled to optimize line capacity (selecting Train A as the leader). The roles have already been defined in the tactical layer, now their operational roles are defined as follows. Initially, when Trains A, B, and C are coupled to optimize line capacity, and the direction is known, as can be seen in Figure 41; The tail of Train A is the master of Train B. The head of Train B is the slave of Train A. The tail of Train B is the master of Train C, and the head of Train C is the slave of Train B.

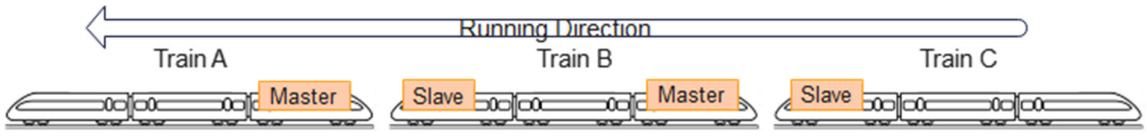

Figure 41: Master-Slave role example. Source: Indra Sistemas S.A

In contrast to the roles in the tactical layer, where there can only be one leader and the rest are followers, the same does not occur in the operational layer, since it is a local role, there must be as many masters and slaves as there are virtual couplings between consist. For a generic use case where there are N consists that are going to be part of the platoon, there are N - 1 virtual couplings and therefore N - 1 master and N – 1 slave. As can be seen Figure 41, if there are 3 trains in the composition there are 2 connections and therefore there are 2 master and 2 slave which are determined automatically due to the running direction.

5.1.1.5 Use Case examples

The following examples of use cases are proposed to define the roles in each of them and to detail their behaviour:

- Use Case – 1: Maximum capacity

For this first case, a strategy based on maximizing capacity is defined, defining the following strategy. There are two trains, Train A and Train B, and the Madrid-Barcelona line. Train A makes stops along the entire line, while Train B runs directly from Madrid to Barcelona.

Train A has the following schedule:

Origin	Departure from origin	Destination	Arrival time at destination
Madrid	7:00 am	Guadalajara	7:30 am
Guadalajara	7:45 am	Calatayud	8:30 am
Calatayud	8:45 am	Zaragoza	9:30 am
Zaragoza	9:45 am	Barcelona	11:30 am

Table 4: Use Case – 1. Train A schedule.

Train B has the following schedule:

Origin	Departure from origin	Destination	Arrival time from destination
Madrid	8:10 am	Zaragoza	9:40 am

Zaragoza	10:00 am	Barcelona	11:30 am

Table 5: Use Case – 1. Train B schedule.

Train A arrives in Zaragoza on track 1 and in Barcelona on track 1 as well. On the other hand, Train B arrives in Zaragoza on track 1 and in Barcelona on track 2.

To meet the schedule and optimize the Zaragoza-Barcelona branch, a coupling manoeuvre is scheduled to be executed on this branch between Trains A and B, with the operating rule of maximizing line capacity. At the same time, to ensure that Train A arrives in Barcelona on track 1 and Train B on track 2, an uncoupling manoeuvre is scheduled between these trains in the area 20-25 km before arriving at Barcelona station.

When both trains A and B are at the Zaragoza station, Train A departs first at 9:45, followed by Train B at 10:00 on the same track 1. To meet the defined strategic objectives, the tactical layer begins generating movement directives for Train A and Train B. Thus, Train A and Train B begin to communicate and decide, based on the characteristics of the operation, that Train A will be the leader and Train B the follower (Figure 42). In turn, in the operational layer, once the direction and number of couplings have been defined, the number of master-slave pairs can be defined (in this case, N-1 = 2-1 = 1 pair) and which train will be the master and which the slave. The tail of Train A will be the master of Train B, and the head of Train B will be the slave of Train A (Figure 42).

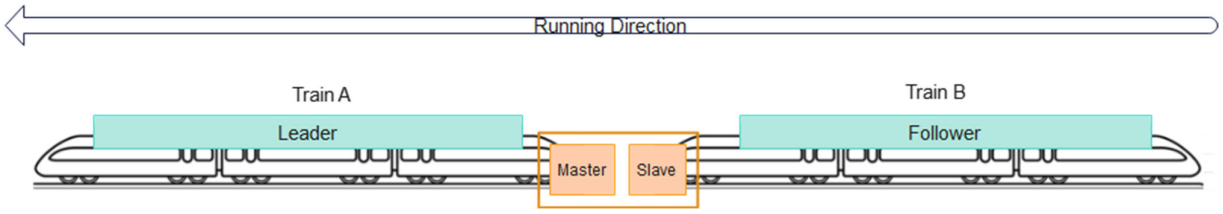

Figure 42: Role Use Cases – 1. Source: Indra Sistemas S.A.

The tactical layer, following the strategy of making a coupling on the Zaragoza-Barcelona branch between Train A and Train B, decides that the coupling should be made as soon as possible, 7 km after leaving the Zaragoza station. The leader (Train A) begins generating movement directives for the coupling to occur. Train B must accelerate to reach a minimum distance to be able to couple with Train A. The operational layer executes these directives.

When the coupling of Train A and Train B takes place, the tactical layer informs the strategic layer and continues generating movement directives (maintaining the coupling based on a minimum distance). The operational layer executes the directives, considering the safety distance. If for safety reasons the coupling cannot be maintained, at the operational layer, the master and slave execute their security guidelines, and an emergency uncoupling occurs.

Maximizing line capacity involves (on the tactic definition implementation) not only maintaining the minimum possible distance, but also coupling as early as possible and uncoupling as late as possible. Therefore, to comply with this strategy and allow Train A to enter Barcelona via Track 1 and Train B via Track 2 and comply with the operational rule of optimizing the line, the tactical layer decides to uncouple 22 km before reaching Barcelona station. This is within the designated area (20-25 km before arriving at Barcelona station), but it attempts to maximize the coupling time. To do this, the leader generates new movement directives, once accepted, the entire convoy then implements the directive in a coordinated manner and at the same time and so that the operational layer can execute them. Train B decelerate to uncouple from Train A.

Once the uncoupling occurs, the tactical layer informs the strategic layer that Train A is uncoupled from Train B and that the switch from Track 1 to Track 2 can be made to enter the Barcelona station.

- Use Case – 2: Energy saving

In the second proposed use case example, there are four trains detailed below (Figure 43) with the following strategy.

Train A is a regional train that runs from Seville to Barcelona with intermediate stops. It has the following schedule:

Origin	Departure from origin	Destination	Arrival time from destination
Seville	6:00 am	Córdoba	7:00 am
Córdoba	7:15 am	Ciudad Real	8:30 am
Ciudad Real	8:45 am	Madrid	10:00 am
Madrid	10:15 am	Zaragoza	12:00 pm
Zaragoza	12:15 pm	Barcelona	2:00 pm

Table 6: Use Case – 2. Train A schedule.

Train B also runs from Seville to Barcelona, but its schedule includes fewer stops:

Origin	Departure from origin	Destination	Arrival time from destination
Seville	8:00 am	Madrid	9:45 am
Madrid	10:00 am	Zaragoza	12:00 pm
Zaragoza	12:15 pm	Barcelona	2:00 pm

Table 7: Use Case – 2. Train B schedule.

Train C travels from Ciudad Real to Barcelona, with the following timetable:

Origin	Departure from origin	Destination	Arrival time from destination
Ciudad Real	9:00 am	Barcelona	2:00 pm

Table 8: Use Case – 2. Train C schedule.

Finally, Train D travels from Valencia to Barcelona, with the following stops:

Origin	Departure from origin	Destination	Arrival time from destination
Valencia	10:00 am	Zaragoza	11:45 am
Zaragoza	12:00 pm	Barcelona	2:00 pm

Table 9: Use Case – 2. Train D schedule.

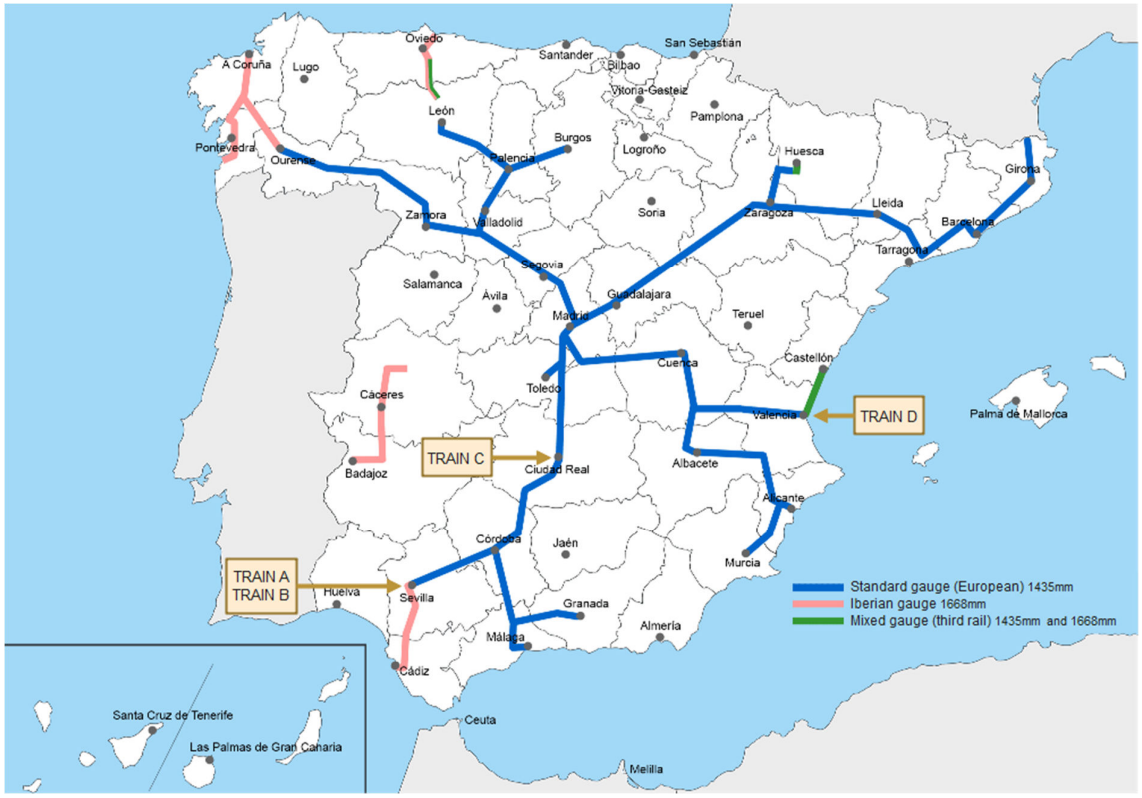

Figure 43: Map Use Cases – 2. Source: Indra Sistemas S.A.

The strategic layer defines that Train A must couple with Train C upon leaving the Ciudad Real station, and Train A must be the leader (Figure 44). It also determines that Train B must couple with the coupled platoon of Train A and Train C upon leaving the Madrid station. In this case, Train B is the leader (Figure 45). Finally, the strategic layer defines that Train D must couple with the platoon formed by Train B, Train A, and Train C upon leaving Zaragoza (Train B remains the leader), arriving at Barcelona station as a single convoy at 2:00 p.m. (Figure 46). All of this follows the operational rule of energy saving.

The main objective of this strategy is to grant - based on VCTS capabilities - the four trains timetable, minimizing the energy consumption, so the tactical layer, to achieve this, tries to take advantage of train synchronization, movement inertia, and regenerative braking. It seeks to reduce unnecessary acceleration and optimize the power usage of the coupled trains.

Initially, the tactical layer focuses on Train A and Train C, as they are the first to be coupled. Train A assumes the role of leader, and Train C of follower. Upon leaving Ciudad Real, the tactical layer begins generating movement directives (the leader) to successfully couple Train A with Train C. Train C must synchronize its acceleration with Train A's speed to minimize energy use during the coupling. The operational layer executes the directives, and Train C couples with Train A at 9:10 a.m. Once the coupling occurs, the tail of Train A becomes the master, and the head of Train C becomes the slave (Figure 44). At this point, the tactical layer generates new directives to maintain the coupling at a distance that allows the operational rule of energy saving and informs the strategic layer that the coupling has occurred and is fulfilling the established plan.

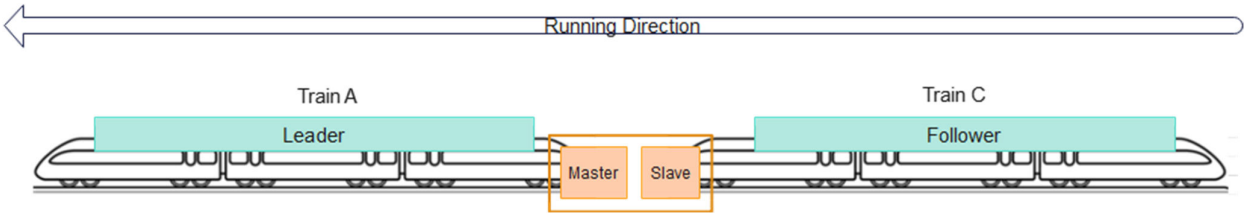

Figure 44: Role Use Cases – 2 (part 1). Source: Indra Sistemas S.A.

The next step of the tactical layer, upon arriving in Madrid, is to communicate the coupled platoon (Trains A and C) with Train B. A consensus is reached that, to pursue the strategic objectives, Train B is the chosen leader, due to it is the one in the head. Therefore, Train A becomes the follower and Train B is the new leader (fulfilling the strategy). Then, to allow the coupling between these trains to take place upon leaving the Madrid station, the leader begins to generate new movement directives. That is, Train B decelerate slightly to align with the platoon (controlled speed to minimize braking), and the platoon of Train A and Train C accelerate to synchronize with Train B. This way Train B successfully couple to the head of the platoon. At this point, a new master (tail of Train B) and a new slave (head of Train A) are defined (Figure 45).

The strategic layer is informed by the tactical layer that the coupling has taken place leaving the Madrid station, complying with operational rules and ensuring compliance with the strategic plan and the distances and times required by the signalling system. The tactical layer continues to generate movement directives to maintain platoon coupling at a safe distance and allow for energy savings.

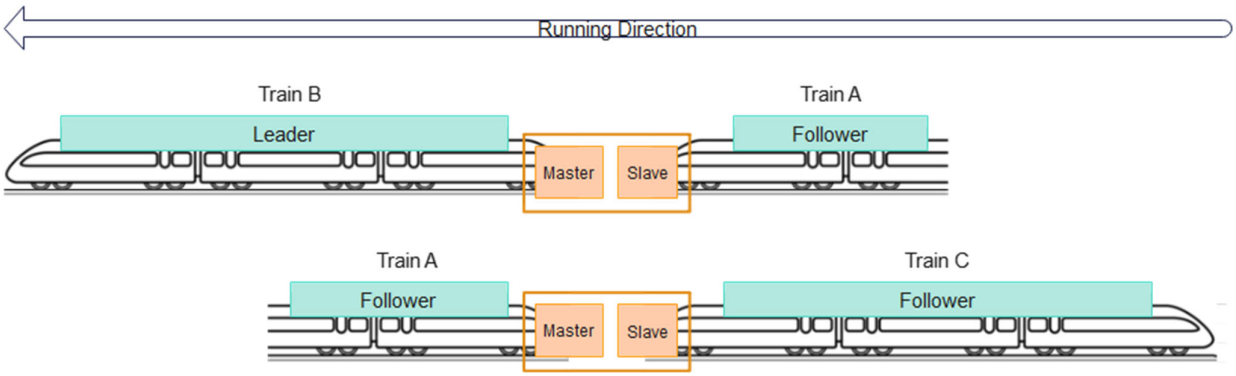

Figure 45: Role Use Cases – 2 (part 2). Source: Indra Sistemas S.A.

For the third coupling defined in the strategy to occur, the tactical layer must communicate the platoon and its coupling with Train D upon exiting Zaragoza. The leader remains on Train B (still the head), and the others assume the role of followers. The operational layer executes the new movement directives generated by the tactical layer. That is, upon exiting Zaragoza, Train D must modulate its speed, accelerating to synchronize with the speed of the convoy. The convoy thus remains unchanged, avoiding sudden braking or acceleration and allowing for energy savings. Once Train D has been coupled to the tail of the platoon, the tail of Train C becomes the master of the new coupling, and the head of Train D becomes the slave. In this way, the entire platoon is now coupled, as seen in Figure 46, where Train B remains the leader, generating movement directives to maintain a safe coupling, with distances and operations that allow for energy savings, and with 3 virtual couplings (and therefore 3 master-slave pairs).
The strategic layer is informed of the coupling by the tactical layer and checks compliance with the timetable.

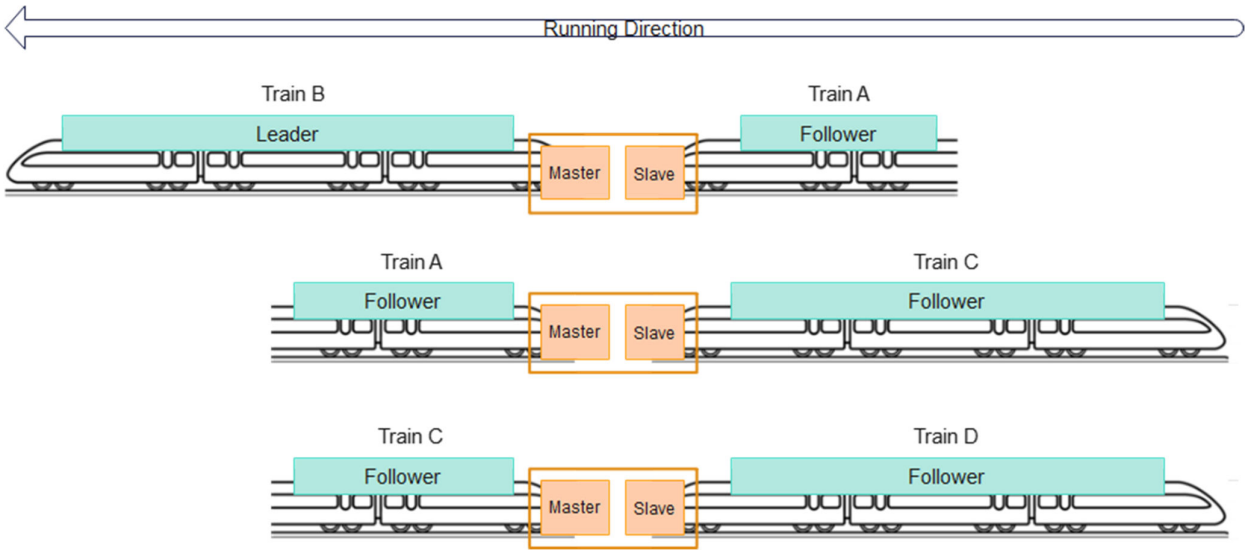

Figure 46: Role Use Cases – 2 (part 3). Source: Indra Sistemas S.A.

The platoon arrives coupled at the Barcelona station at the established time, 2:00 p.m.
In this way, it can be observed how the tactical layer seeks to optimize energy by minimizing braking and acceleration and coupling the trains as quickly as possible (energy expenditure is reduced on the route in which the trains are coupled, especially on the final route, when only one platoon is connected).

- Use Case – 3: Complex use case, energy saving and minimum distance

In this case, the following strategy is defined. There are three trains: Operator 1 Train A, Operator 2 Train B, and Operator 3 Train C. Train A goes to Seville and departs from Atocha on track 2 and stops in Puerto Llano. Train B goes to Seville directly and Train C goes to Córdoba directly. Both (Train B and C) depart from Atocha on track 1 at 11:30 am, 2:30 hours after Train A (Figure 47). The operational rule imposed by the railway operators is energy saving, while the railway administrator sets the operational rule of maximum capacity.

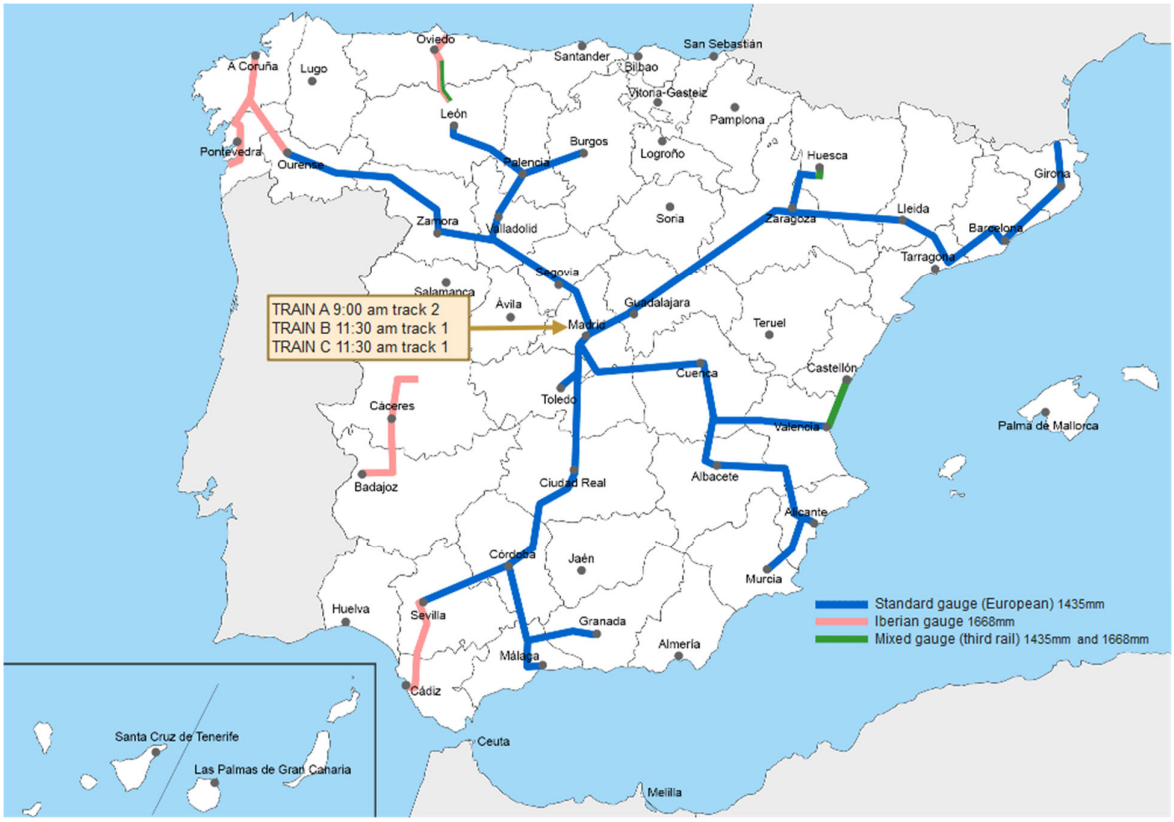

Figure 47: Map Use Cases – 3. Source: Indra Sistemas S.A.

Train B and C must be coupled between Atocha and Puerto Llano (Figure 48). Train A arrives in Puerto Llano, stops for 15 minutes, and departs for Córdoba. It must be coupled with Train B and Train C between Puerto Llano and Córdoba (Figure 49). Before reaching the Córdoba bypass, Train A and Train B must uncouple from Train C without stopping in Córdoba and continue to Seville (Figure 50). While Train C must uncouple to stop in Córdoba.

The tactical layer, in the first instance, already knows the strategic objectives and operational rules, and therefore generates an associated tactic to achieve them. The first step is to try to couple Trains B and C between Atocha and Puerto Llano as soon as possible, to comply with the line optimization requirements (the railway administrator's operational rule). It will then try to ensure that when both trains are coupled, the distance between them is compatible with energy savings, thus complying with the operators' energy saving rule.
The same will occur when the coupling between Train A and Trains B and C (between Puerto Llano and Córdoba) is required. The tactical layer will seek to complete the coupling as soon as possible. Once this occurs, it will check that the distance between the three trains is compatible with energy savings. In turn, to comply with the administrator's operational rule, when the uncoupling is required, the tactical layer will seek to uncouple the trains as late as possible, close to the Córdoba bypass,

to maximize the line's capacity. This way, it is possible to optimize the management of the train paths much more, allowing three trains to fit into the same path.

To couple, Train B and Train C, they first communicate with each other and reach a consensus that Train B, being the one in the head, will be the leader. In the tactical layer, the leader generates new movement directives for the coupling to occur: Train B must maintain its speed, and Train C must accelerate and couple with Train B. The operational layer executes these movement directives. Once the coupling between Train B and C occurs, the master (tail of Train B) and slave (head of Train C) are defined in the operational layer (Figure 48). The tactical layer informs the strategic layer that the coupling has been successful and generates new directives to maintain the coupling at a distance that allows for energy savings.

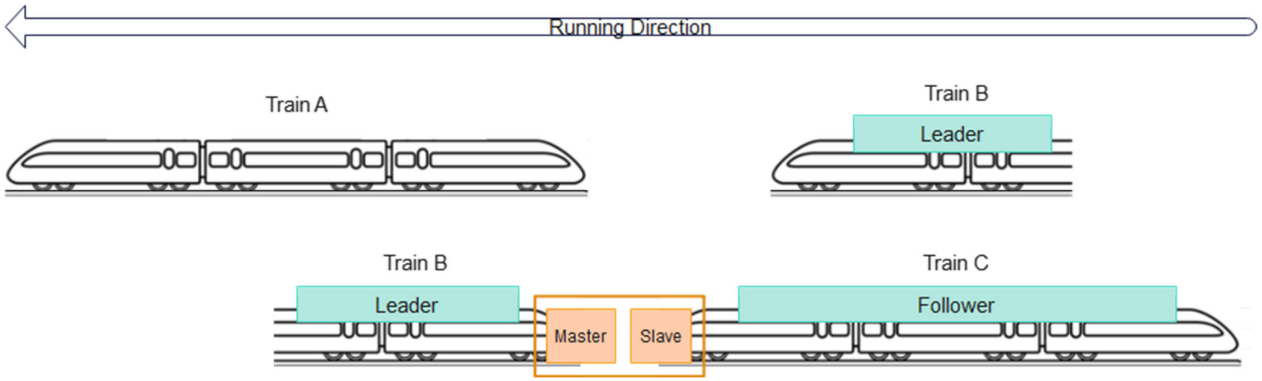

Figure 48: Role Use Cases – 3 (part 1). Source: Indra Sistemas S.A.

Upon passing the Puerto Llano station, the tactical layer begins generating new movement directives: Train A must couple with the platoon. The three trains communicate with each other, and it is decided to transfer the leader to Train A, since it will be the head train. Train A becomes the leader, Train B becomes the follower, and Train C still follower. For the coupling to occur, the operational layer executes the new movement directives: accelerate Train B to be able to couple with Train A. Train C, being Train B's slave, does the same as Train B.
When the coupling occurs, the tail of Train A assumes the role of master, the head of Train B becomes the slave, and everything else remains the same (Figure 49). Again, the tactical layer informs the strategic layer that the coupling has occurred and generates new directives to maintain the coupling at a distance that allows for energy savings. At the same time, the line has also been optimized with the couplings.

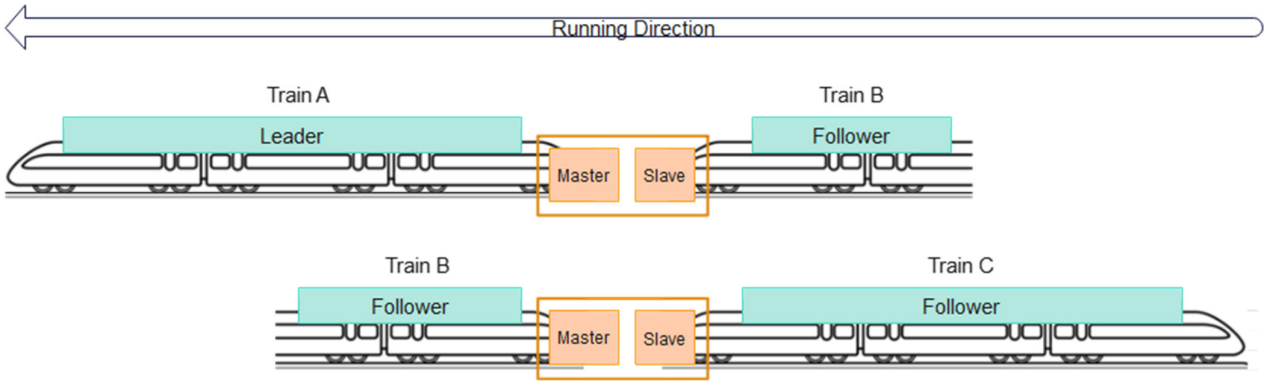

Figure 49: Role Use Cases – 3 (part 2). Source: Indra Sistemas S.A.

Before reaching the Córdoba bypass, the tactical layer, to meet the objectives and time requirements, decides that Train C must uncouple 5 km before reaching the bypass. To do so, Train A maintains the platoon lead, and the tactical layer generates directives to carry out the uncoupling. The operational layer executes these directives, increasing the distance between Train C and Train B, and the uncoupling is completed (Figure 50). The tactical layer ensures that Train C can switch the track and stop in Córdoba and reports to the strategic layer. The platoon now consists only of Train A and Train B, which continue until they stop in Seville.

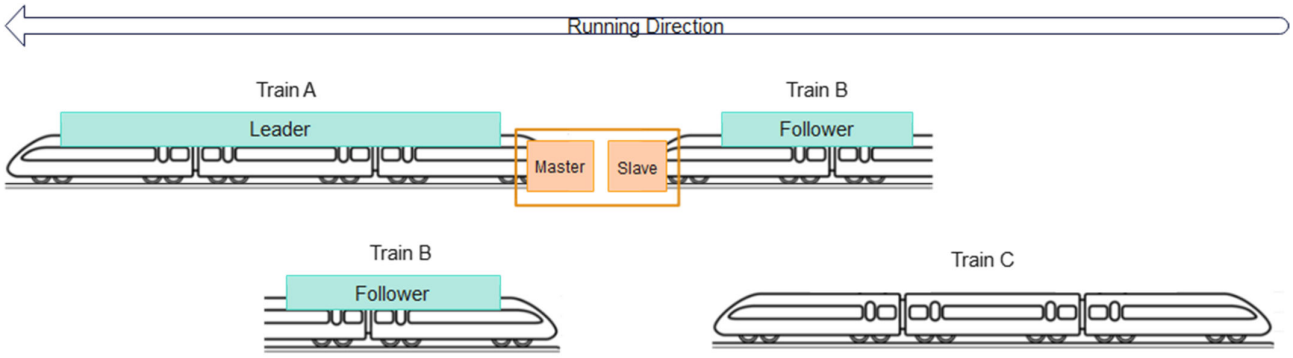

Figure 50: Role Use Cases – 3 (part 3). Source: Indra Sistemas S.A.

5.1.2 Tactical layer model

To simulate Virtual Coupling, a Python multi-train simulation tool developed at DLR was used. This multi-train simulation uses forward-propagating dynamics: starting from the initial states of the system, the model calculates subsequent states over a series of time steps using known equations of dynamics.

Figure 51 shows the build-up of the model. Object oriented approach is used to capture the characteristics of different components and actors of the system along with the environment it interacts with. The simulation allows the multiple trains to be defined with different characteristics to simulate a mixed platoon. The Train model consists of several submodules that represent different components and attributes of trains including environment, dynamics, powertrain, tactical layer and operational layer which interact with each other to simulate VCTS as shown in Figure 51.

.

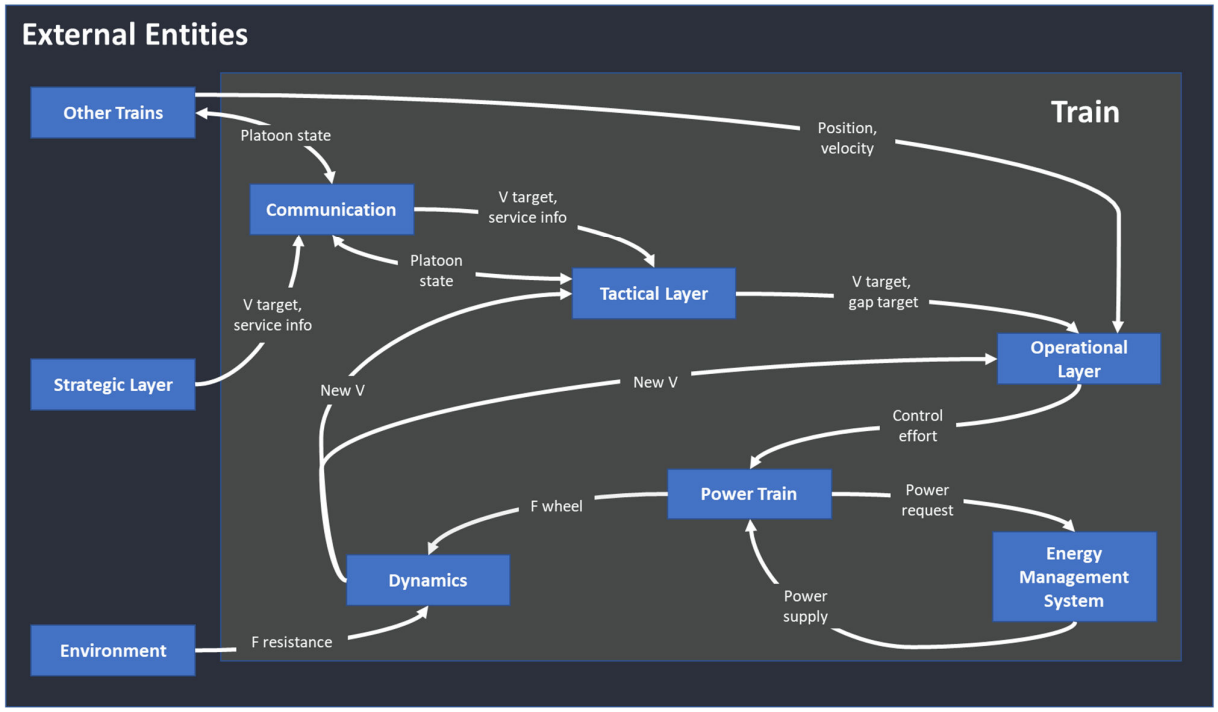

Figure 51: Multi train simulation flow

5.1.2.1 Environment

The environment module allows the user to define the track layout and parameters, such as gradient. This is used by the multi train simulation model to calculate the resistance forces acting on the train and the resulting dynamics. To calculate the resistance acting on the trains the Davis resistance model is used. The resistance force acting on the train calculated as follows:

$$\boldsymbol{F}_{resistance} = \boldsymbol{A} + \boldsymbol{B}\boldsymbol{v} + \boldsymbol{C}\boldsymbol{v}^{\boldsymbol{2}} + \boldsymbol{F}_{gradient} \quad (1)$$

where A, B and C are constant characteristics of the train and v is the velocity of the train. A is the coefficient of rolling mechanical resistance. B is the mechanical resistance (brake drag, transmission losses, etc.) and the air momentum drag, as well as various other resistances such as the one due

to ventilation. C is coefficient of aerodynamic resistance, which depends on the geometry of the train [118]. F_{gradient} is the force acting on the train due to inclination of the track given by:

$$\boldsymbol{F}_{gradient} = \boldsymbol{mg\ sin\ \theta} \tag{2}$$

where m is the mass of the train, g is the acceleration of gravity and θ is the inclination angle in radians.

5.1.2.2 Dynamics

The dynamics module is used to calculate the change in states of the trains at each time step based on the forces acting on the train. The model only considers longitudinal dynamics and the train is treated as a point mass.

The total effective force acting on a train at any given time is:

$$\boldsymbol{F}_{effective} = \boldsymbol{F}_{wheel} - \boldsymbol{F}_{resistance} \tag{3}$$

where F_{wheel} the force acting on the wheels of the train, which is controlled by the driving or braking force from the train and $F_{\text{resistance}}$ is calculated by the environment module at each time step. Applying newtons second law of motion for any given time k we get

$$\boldsymbol{F}_{effective,k} = \boldsymbol{m'} \cdot \boldsymbol{a_k} \tag{4}$$

$$\boldsymbol{a_k} = \frac{\boldsymbol{F}_{effective,k}}{\boldsymbol{m'}} \tag{5}$$

where m' is the mass of the train and $\mathrm{a_k}$ is the acceleration at time k. The subsequent states of the train are calculated and updated over each time step $\mathrm{k}+1$ as:

$$\boldsymbol{v_{k+1}} = \boldsymbol{v_k} + \boldsymbol{a_k \Delta t} \tag{6}$$

$$\boldsymbol{s_{k+1}} = \boldsymbol{s_k} + \boldsymbol{v_k \Delta t} \tag{7}$$

Where v is the velocity of the train and s is the position of the train. To simulate other environmental influences on trains, stochastic variable such as wind and disturbances from the track have been included in the environmental module, which will be discussed in more detail in chapter 5.2.2

5.1.2.3 Powertrain

This module captures powertrain characteristics of the train. It is to be noted that the powertrain losses are not considered here. The powertrain module receives the desired driving effort/control effort (u) from the operational layer of the train. This is used to calculate the power desired (P_{des}) to be delivered by the powertrain to achieve driving effort demanded by the operational layer, as follows

$$\boldsymbol{P_{des,k}} = \boldsymbol{P_{max}} \cdot \boldsymbol{u_k} \tag{8}$$

$$\boldsymbol{P_{max}} \in [-\boldsymbol{P_{br}}, \boldsymbol{P_{dr}}] \tag{9}$$

where P_{max} represents the maximum braking and driving power available at the wheels. Which is constrained by maximum available braking power (P_{br}) and maximum driving power (P_{dr}). The maximum braking and driving power are constant in the model. Once the target power is calculated,

the power is to be requested from the energy management system as shown in Fig. 3.5. The power to be requested $P_{req,k}$ is calculated as follows

$$\boldsymbol{P}_{req,k+1} = \boldsymbol{P}_{req,k} + \frac{(\boldsymbol{P}_{t,k} - \boldsymbol{P}_{req,k})\boldsymbol{\Delta t}}{\boldsymbol{\tau}} \quad (10)$$

To model the delay between the powertrain receiving the requested power and responding to the request, a first order time delay (τ) is introduced. If the requested power is available, f_{wheel} is calculated from the power that is requested.

$$\boldsymbol{f}_{\boldsymbol{wheel},\boldsymbol{k}} = \frac{\boldsymbol{P}_{supply,k}}{\boldsymbol{v}_{\boldsymbol{k}}} \quad (11)$$

where $P_{supply,k}$ is the power supplied by the energy management system. The force that can be supplied to wheels is constrained by the adhesion limits between wheel and track and strength of the powertrain components involved. Therefore, it is constrained within f_{max}.

$$|\boldsymbol{f}_{\boldsymbol{wheel}}| \leq |\boldsymbol{f}_{\boldsymbol{max}}| \quad (12)$$

5.1.2.4 Energy Management

The energy management module represents the energy source and energy management system of the train. It receives the power request $P_{req,k}$ from the power train module and supplies the power if available. A simplified battery model is used as source of energy in this model to keep track of the energy usage. If the State of Charge (SOC) of the battery is not depleted the energy management supplies the powertrain with the requested power and the SoC is updated each time step.

$$\boldsymbol{P}_{req,\boldsymbol{k}} = \boldsymbol{P}_{supply} \quad if \quad SoC > \boldsymbol{0} \quad (13)$$

$$SoC = SoC_{\boldsymbol{0}} - \boldsymbol{P}_{req,\boldsymbol{k}} \cdot \boldsymbol{\Delta t} \quad (14)$$

5.1.2.5 Strategic Layer

In this model the strategic layer partially encapsulates functions of the service layer of VCTS as well. It defines the service for each train, including schedules, stop locations, which trains need to couple or decouple, and where each manoeuvre should be executed.

5.1.2.6 Communication layer

This module represents the communication channel between the trains. It enables the tactical layers of different trains to send messages to each other as shown in Figure 51. The messages may contain information such as current states of trains, coupling status, train ID's and braking curves. It is also used to receive information from the strategic layer regarding services and to communicate platoon states. There is a probability that messages can drop out due to disturbances in the communication channels due to environmental factors which is a critical aspect to be considered during VCTS manoeuvres. This is discussed in more detail in chapter 5.2.3

5.1.2.7 Tactical layer

This module coordinates platoon movements within a VCTS and is responsible for assigning roles to individual consists, designating them as leaders or followers. It interacts with the strategic layer to

retrieve information about the service being carried out, including speed limits, optimal speed profile, details on upcoming VCTS manoeuvre such as which the id's of trains that need to couple or decouple, along with the location of these operations.

Additionally, the tactical layer of the leader trains issues directives to the platoon, specifying inter-vehicular distances to maintain and providing instructions for coupling and decoupling manoeuvre based on specific scenarios. Since the manoeuvre are executed locally by the operational layer, the tactical layer also transmits the necessary commands to ensure proper execution at the operational level.

5.1.2.8 Operational layer

This represents the local control of the train. It interacts with the powertrain module and tactical layer of the train as shown in Figure 51. It receives commands and state information, speed limits etc. of adjacent trains from the tactical layer to control the dynamics of the train. The operational layer has two control modes the trajectory following control and gap control mode.

Trajectory following control: When trains are driving independently they use a trajectory following control. This control receives a velocity trajectory that is optimized for minimum energy usage, as developed in [119], as reference. In a virtually coupled scenario the leader train also uses the optimized velocity as reference. A multivariable feedback control (MFC) is used to follow the trajectory using the following equation:

$$\boldsymbol{F_{target}(t) = k_1 \cdot \left(a_{opt}(t) - a_{actual}(t)\right) + k_2 \cdot \left(v_{opt}(t) - v_{actual}(t)\right) + k_3 \cdot \left(s_{opt}(t) - s_{actual}(t)\right)} \quad (15)$$

Where the variables a, v and s are the acceleration, velocity and position. The control parameters $k_{1\ldots3}$ are optimized by minimizing the loss function which, besides the energy, includes penalties for not stopping at the right moments, exceeding the speed limit, and arriving late at the stations.

$$\boldsymbol{J(s_{actual}, v_{actual}, F_{wheel}, k_{1..3}) = \int_{t_0}^{T} F_{wheel}(t) \cdot v_{actual}(t) + c_1 \cdot max\left(0, v_{actual}(t) - v_{limit}(t)\right) + c_2 \cdot P_{stop}(t)\, dt + c_3 \cdot max\left(0, s_{actual}(T) - s_{opt}(T)\right) + c_4 \cdot |k|} \quad (16)$$

where $|k|$ denotes the L2-norm of the control parameters, and the coefficients $c_{1\ldots3}$ represent the weight of the penalty for respectively exceeding the speed limit, not stopping at the station at the proper time, not finalizing the service at the proper time, and the regularization of the control weights.

Gap control: When trains need to be virtually coupled or decoupled, they must communicate their states and braking curves to each other to adjust the gap between them—from distances greater than ABD to those close to RBD, and vice versa. A gap control is built into the simulation for such manoeuvre. For the gap control, a sliding mode controller (SMC) is used, due to its robustness to deal with disturbances and uncertainties in the system.

The train responsible for controlling the distance to the adjacent train receives the states of the adjacent train and has access to its own state, which are then used to calculate the control effort required u. The SMC gap controller is designed by defining a sliding surface that represents the desired system dynamics. This sliding surface incorporates the errors in position and velocity of the

follower train relative to the leader train. The communication between trains and sensor accuracy is so far assumed ideal: i.e. no communication loss, delays, or inaccuracies.

The control law used in the sliding mode follows:

$$\boldsymbol{u(t)} = \frac{\boldsymbol{K} \cdot \big(\boldsymbol{\sigma(t)}\big)}{\big|\big(\boldsymbol{\sigma(t)}\big)\big| + \boldsymbol{\rho}} \tag{17}$$

where K is the controller gain and ρ the boundary parameter. This control law drives the system in the opposite direction of the error, aiming to eliminate it by bringing the state closer to the surface σ. The boundary layer method is applied to the control signal $u(t)$ to mitigate chattering phenomena. This method helps stabilize the control action.

The sliding surface $\sigma(t)$ is defined as:

$$\boldsymbol{\sigma(t)} = \boldsymbol{e_s(t)} + \boldsymbol{\lambda} \cdot \boldsymbol{e_v(t)} \tag{18}$$

$$\boldsymbol{\sigma(t)} = \boldsymbol{s_{leader}(t)} - \boldsymbol{s_{follower}(t)} - \boldsymbol{t_{target}} \cdot \boldsymbol{v_{follower}(t)} + \boldsymbol{\lambda} \cdot \Big(\boldsymbol{v_{leader}(t)} - \boldsymbol{v_{follower}(t)}\Big) \tag{19}$$

where $e_s(t)$ and $e_v(t)$ are the error in position and velocity w.r.t the leader train, λ is a gain factor, and t_{target} is the desired gap expressed in time. This sliding surface is employed when trains are coupled.

For the coupling and decoupling phases, the SMC uses an Adaptive Time Headway (ATH) method, similar to the method proposed by [120], to smoothly converge the gap to desired gap. It aims to prevent excessive overshoot resulting from uncontrolled correction effort and to achieve asymptotic convergence of the gap and relative speed.

This method divides the approach manoeuvre of the gap-responsible train into two phases. The parameter $t_{critical}$ determines the end of phase 1 and start of phase 2. During phase 1, the sliding surface $\sigma_1(t)$ is expressed as:

$$\boldsymbol{\sigma_1(t)} = \boldsymbol{e_s(t)} - \big(\boldsymbol{t_{carrot}(t)} \cdot \boldsymbol{v_{actual}(t)}\big) \tag{20}$$

To guarantee a smooth transition from the ABD to RBD, the sliding surface is manipulated using an additional carrot headway $t_{carrot}(t)$. The $t_{carrot}(t)$ is initialized at t_0 when the coupling procedure starts, as the difference between the current headway and the target one. Then the carrot headway is asymptotically reduced to zero to achieve the target gap smoothly. The rate at which the carrot headway is reduced in phase 1 is as follows

$$\boldsymbol{t_{carrot}(t_0)} = \frac{\boldsymbol{e_s(t_0)}}{\boldsymbol{v_{actual}(t_0)}} \tag{21}$$

$$\boldsymbol{t_{carrot}(t+1)} = \boldsymbol{t_{carrot}(t)} - \frac{\boldsymbol{K} \cdot \boldsymbol{t_{critical}} \cdot \boldsymbol{\Delta t}}{\boldsymbol{v_{actual}(t)}} \tag{22}$$

The rate at which t_{carrot} is reduced is determined by parameter K. The parameter $t_{critical}$ scales the rate at which t_{carrot} is reduced according to the length of phase 2. For example, if t_{carrot} is large the gap convergence can be faster, since phase 2 is larger which implies the gap to partner train is large. Furthermore, the rate at which the t_{carrot} is reduced is also inversely proportional to the actual speed of the train. Which means with the increasing speed of the train, the rate at which the gap is converged is slowed down.

Once the follower train reaches a specified headway $t_{critical}$, which is close to the desired gap, phase 2 begins. In this phase, a different sliding surface is utilized to facilitate smooth asymptotic convergence to the final desired gap. In phase 2, the sliding surface σ_2 is:

$$\boldsymbol{\sigma_2 = e_s(t) - t_{carrot}(t) \cdot v_{actual}(t) + \left(t_{critical} - t_{carrot}(t)\right) e_v(t)} \quad (23)$$

The difference between the sliding surface σ_1 and σ_2 is that σ_2 also considers the $e_v(t)$, which is the relative speed. This enables more precise control and asymptotic gap convergence. The rate at which the carrot headway is reduced in phase 2 is as follows

$$\boldsymbol{t_{carrot}(t+1) = t_{carrot}(t) - t_{carrot}(t) \cdot \frac{K \cdot \Delta t}{v_{actual}(t)}} \quad (24)$$

However, in order to limit the relative velocity between the trains, a third sliding surface σ_3 is enabled if the relative velocity exceeds a specified limit $v_{rel,max}(t)$:

$$\boldsymbol{\sigma_3(t) = v_{leader}(t) - v_{follower}(t) - v_{rel,max}(t) \quad \text{if} \quad \left|v_{leader}(t) - v_{follower}(t)\right| > v_{rel,max}} \quad (25)$$

With the ATH based SMC gap control the trains are able to couple and decouple smoothly, ensuring relative speeds are limited and safe. An example simulation of a coupling, coupled driving and decoupling manoeuvre is shown below in Figure 52

It is to be noted that the gap controls were tuned heuristically. There is room for optimization of the controls for better energy efficiency of the platoon as a whole.

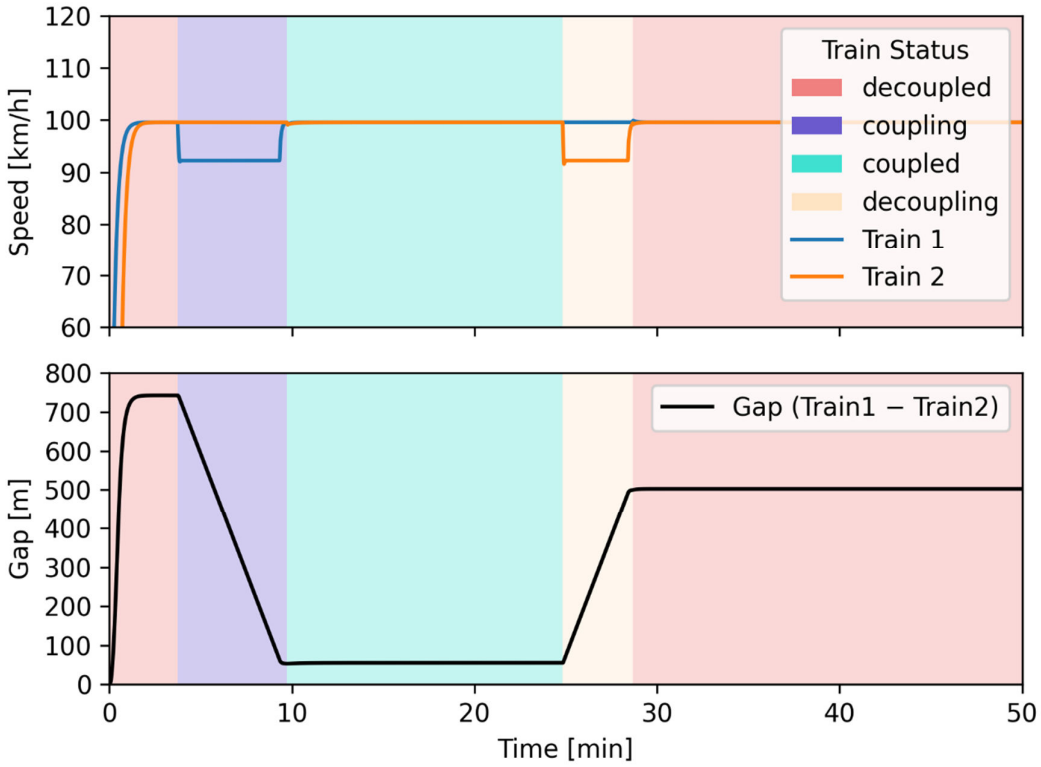

Figure 52: VCTS simulation of coupling and decoupling with a platoon of 2 consists

5.2 ASSESSMENT OF DRIVING STRATEGIES

5.2.1 Driving manoeuvre analysis

Four different modes of VCTS can be simulated in the multi-train simulation model: decoupled, coupling, coupled and decoupling which will be discussed in detail in this subchapter. When and where the manoeuvres are executed is to be determined by the strategic layer. Since, the strategic layer is not the focus of this WP, the sections of the track where the different manoeuvres should take place will be predefined in simulations.

There are various possible strategies to execute these manoeuvres. Depending on the scenario, each have their own advantages and disadvantages which will also be discussed in this chapter. The tactical layer will make the decision of which strategy to follow based on the scenario.

5.2.1.1 Decoupled Mode:

This mode refers to scenario when trains operate independently, following presumably ETCS L2 or ETCS L2 moving block signalling principles. During this state, each train maintains a minimum of absolute braking distance with each other. In this phase no train-to-train communication is established. The trains operational layer has objective to follow the speed trajectories provided by the tactical layer. The trajectory following control in chapter 5.1.2 is active in this phase.

5.2.1.2 Coupling Mode:

When the trains enter coupling mode, the communication between the trains that are planned to be coupled is initiated. The tactical layer receives information from the strategic layer, about which train to interact with and where to execute the manoeuvres.

Depending on the scenario, the tactical layer assigns one of the trains the roles as follows:

Leader: The objective of this train will be continue following the speed trajectory provided by the tactical layer, while communicating its states to the other consists to enable coupling. The trajectory control referred to in chapter 5.1.2 is active on the leader train when it is a part of a VCTS.

Follower: The trains that are planned for platooning are assigned the role of the follower. The follower's objective is to reduce the gap with the train adjacent to them, without violating the speed limits and safety constraints. The gap control from chapter 5.1.2 is active from this phase onwards. The gap controller of the coupling train considers the maximum speed limit of the track to ensure the safety limits are not exceeded. Additionally, the relative speeds of the train are limited gap controller to ensure smooth, controlled and safe execution of the manoeuvres.

Since any consist that is part of a VCTS platoon can be assigned the roles of leader of follower. It is also important to distinguish between the roles and positions of trains in a platoon.

- Train 1 will refer to the train that is driving at the front of the platoon in the direction of travel.
- Train 2,3, 4 etc. will be the trailing consists behind Train 1.

It is also important to note that coupling and decoupling are bidirectional - meaning that either the train in front or the trailing consist can initiate the manoeuvre, and either one can adjust its speed or behaviour to complete it, depending on the situation and strategy selected by the tactical layer.

When talking about VCTS manoeuvre in this chapter, the focus is always on two adjacent consists within a VCTS platoon.

There are two possible strategies to couple two trains and converge the gap between them as shown in Figure 53.

Strategy 1: Train 2 accelerates to Train 1
The first strategy involves Train 2 accelerating to a speed larger than the Train 1 in order to converge the gap and then maintaining the gap.

Advantages:
- The train 1 does not lose any time during the coupling manoeuvre.
- The train 2 gains time freeing up more of the track behind for other trains to occupy and hence increasing throughput.

Disadvantage:
- Bottleneck due to the speed limitations. If the train 1 is already driving at the speed limit of the track, the train 2 will have to drive over the speed limits to converge the distance between the trains which is legally not possible.

Strategy 2: Train 1 slows down for Train 2
The second strategy involves the Train 1 slowing down to converge the gap with the follower safely.

Advantages:
- Unlike in strategy 1, this strategy is that will always be possible regardless of speed limits.

Disadvantage:
- Train 1 loses time, reducing the throughput of the track. However, this manoeuvre could still be useful in scenarios where there are specific timing constraints. e.g. a platoon passing a level crossing within specific duration.

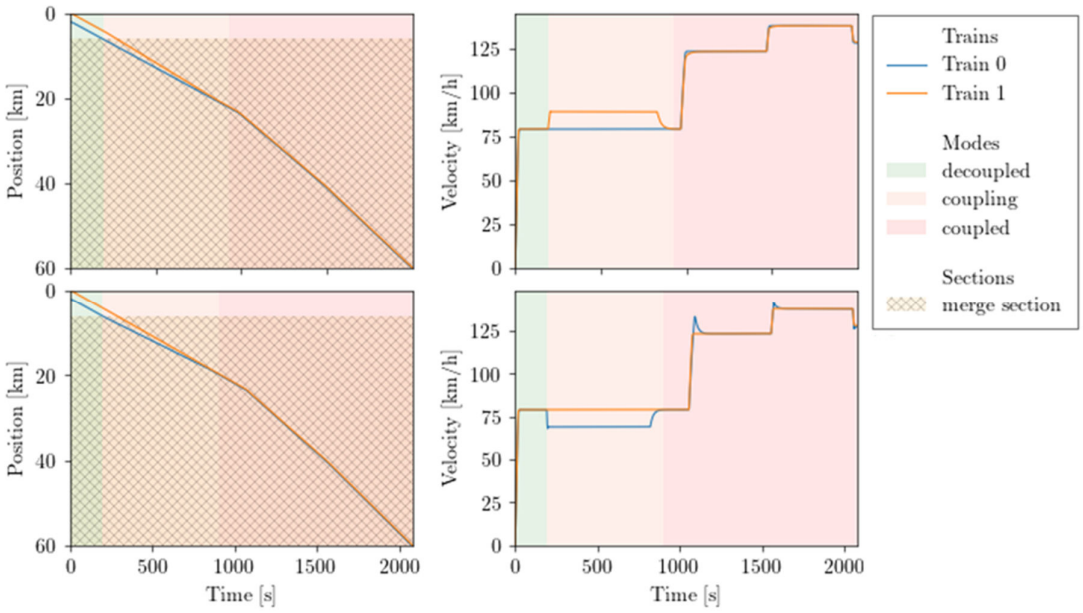

Figure 53: Coupling strategies 1 and 2

5.2.1.3 Coupled Mode

The coupled mode is an extension of the coupling mode. Once the train 2 successfully converges the gap between itself and train 1 or vice versa (depending on chosen strategy) the operational layer checks if the stability conditions are met and switches the mode to coupled. The tactical layer communicates the status with the strategic layer and other trains. Once the trains are in coupled mode they are to be perceived as a single train by the strategic layer and other trains on the track.

5.2.1.4 Decoupling Mode

During the decoupling mode, the tactical layer initiates the process by assigning the train that is decoupling the role of the leader. The target gap for the follower now is set to a distance greater than ABD. During this phase the gap control is active and ensures the same safety constraints such as maximum speed limit of the track and maximum allowed relative speed is not violated and the new target gap is achieved smoothly.

Once the target gap is achieved, the decoupling procedure is complete. The tactical layer then switches the train's mode from decoupling to decoupled. As a result, the train stops communicating with the platoon and continues driving independently, following the reference velocity trajectory provided by the strategic layer. Similar to the coupling mode there are two possible strategies for decoupling the trains as shown in Figure 54.

Strategy 1: Train 2 slows down for train 1
The first strategy involves the train 2 slowing down to a speed lower than the train 1 to increase the gap with the train 1.

Advantages:
- The leading train does not lose any time in the decoupling manoeuvre.

Disadvantages:
- May reduce the track throughput as the follower slows down, potentially affecting the traffic behind.

Strategy 2: Train 1 speeds up for train 2
The second strategy involves the train 1 speeding up to increase the gap with train 2.
Advantages:
- Maintains high track throughput.

Disadvantages:
- May not be feasible if the platoon is driving at speed limit.
- May not be feasible if there is traffic ahead on the same track.

It can be concluded that gains from VCTS in terms of time or capacity therefore, depend on each specific scenario and strategy that is chosen for the manoeuvre in each scenario. The tactical layer can flexibly assign roles and chose strategies based on specific scenarios allowing bi-directional coupling and decoupling. For example, in Figure 52: VCTS simulation of coupling and decoupling with a platoon of 2 **consists** a mixed strategy where train 1 slows down to couple and train 2 slows down to decouple is used.

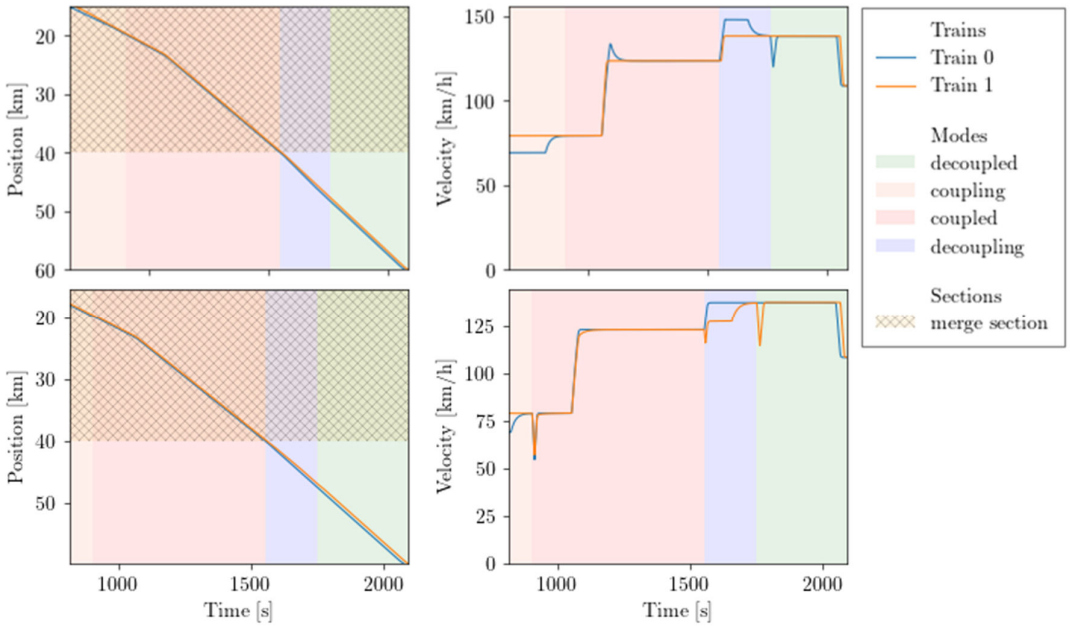

Figure 54: Decoupling strategies 1 and 2

5.2.2 Characterisation of control strategies

As described in chapter 5.1.2.8 a sliding mode gap controller designed for simulation of VCTS gap control manoeuvre. To evaluate its performance under different stochastic influences from the environment various studies were conducted for different manoeuvre.

Impact of external disturbances during coupling and decoupling

To analyse how the gap control performs during the coupling and decoupling manoeuvre a study was conducted in [121]. The study examined the gap overshoot and velocity overshoot of trains coupling and decoupling at varying speeds and relative speeds, under the influence of external disturbances from the variations in gradient profile. The results showed that the controller was able to smoothly converge the gaps to the target gap during both coupling and decoupling, without significant gap or velocity overshoot, even in the most extreme simulated cases, as shown in Figure 55 and Figure 56.

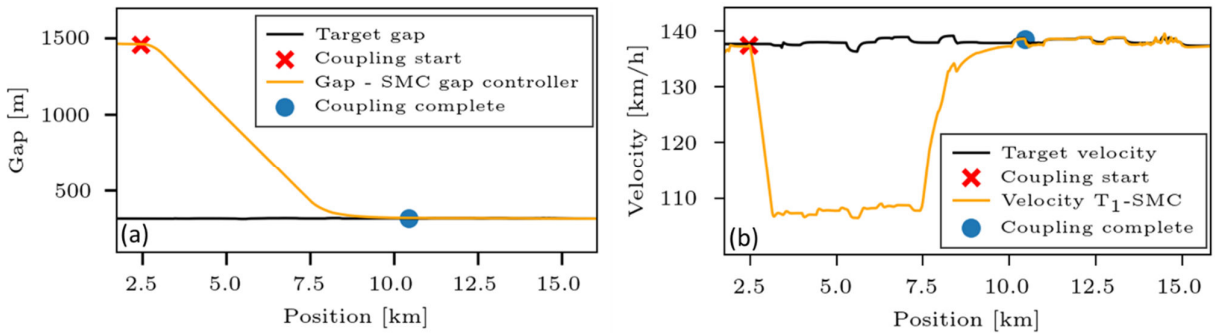

Figure 55: Coupling manoeuvre at 140 km/h and relative velocity 30 km/h

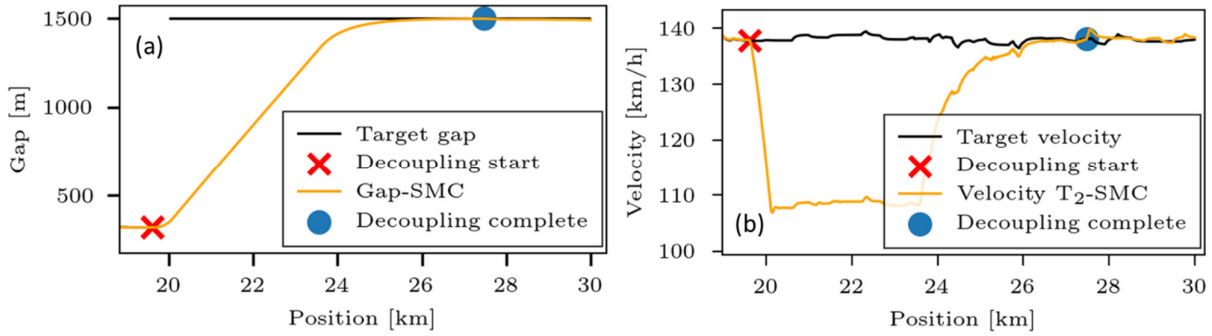

Figure 56: Decoupling manoeuvre at 140 km/h and relative velocity 30 km/h

Energy consumption during coupled driving manoeuvre

In [122] a study is conducted to assess the effectiveness of the gap control during coupled driving manoeuvre in presence of stochastic disturbances from wind resistance and rolling resistance. A gaussian noise generator along with a low pass filter was used to model these external disturbances. The external disturbance is added to the resistance force from equation **(1)** in the environment module to simulate the effects as follows.

$$\boldsymbol{F_{resultant}(t) = F_{wheel}(t) - \left(A + B \cdot v_{actual}(t)\right) \cdot \left(1 + f_{roll}(t)\right) - C \cdot \left(v_{actual}(t) + f_{wind}(t)\right)^2} \qquad (26)$$

where f_{wind} and f_{roll} are the filtered external disturbances that are added to the resistance forces acting on the train.

A service scenario of a platoon with two consists travelling from Hagen-Warburg-Hagen comprising of 34 station. This scenario was chosen because it represents a typical regional line service in Germany.

It was simulated under three different conditions to assess the impact of stochastic variables on VCTS behaviour and gap control.

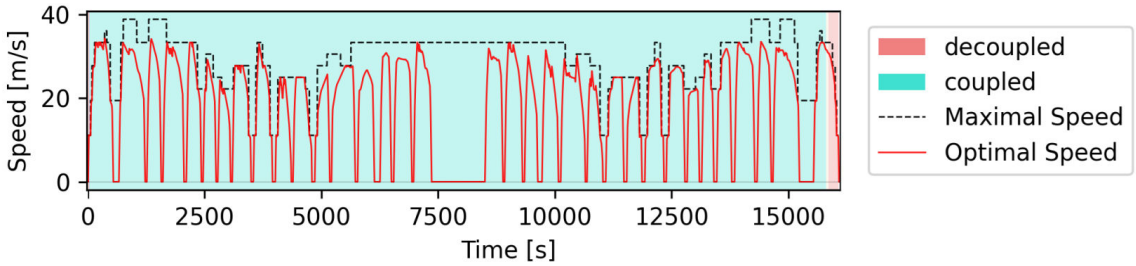

Figure 57: Service scenario Hagen - Warburg - Hagen

Impact of Constant Headwind

First a scenario with various speeds of constant headwind was simulated and the impact on energy required for the consists to complete the service was analysed. Table 10 shows the results of the simulation. The first row in the table shows the baseline energy consumption of both consists of the platoon for this specific service without any additional external disturbance. It can be seen that the energy required by follower train that is trying to maintain the gap with leader is less than 4% higher than the leader train in this scenario. It can also be seen that the difference remains similar even with different varying speeds of headwind introduced to the system.

From the equation **(26)** we know that headwind has a quadratic relation to the resistance acting on the consists. It can also be seen the energy required by the following consists is in the same order of magnitude as the leader. This indicates that the gap controller requires negligible control efforts to maintain inter-vehicular gap in the presence of constant headwinds.

The aerodynamic impact of the consists on each other is not considered in the simulation. However, previous studies done on impact of aerodynamics on VCTS platoons shows that, the aerodynamic benefits of VCTS diminish significantly with increasing inter-vehicular distances. CFD simulations done in [123] revealed that the reduction of drag coefficient of a two-train platoon travelling at 80km/h that had inter-vehicular gaps more than 10m was insignificant.

Wind Speed (km/h)	Leader Energy (MWh)	Follower Energy (MWh)
0.0	776.71 (baseline)	806.36 (baseline)
7.2	793.29 (+2.13%)	822.66 (+2.02%)
14.4	811.24 (+4.45%)	845.94 (+4.91)
21.6	830.49 (+6.92%)	862.27 (+6.93)
28.8	851.12 (+9.58)	882.89 (+9.49%)

Table 10: Headwind Impact on Energy

Impact of Wind Gusts

Since, headwinds are not necessarily constant in a real life, a second scenario with varying wind gust intensity was simulated. In order to simulate this the wind gust intensity with varying standard deviations with mean zero was simulated. Table 11 shows the results of the simulation for different standard deviations of wind speed.

Wind Gust Speed (km/h)	Leader Energy (MWh) ± Std	Follower Energy (MWh) ± Std
14.4	777.52 ± 5.08 (+0.10%)	808.01 ± 5.59 (+0.20%)
21.6	781.93 ± 7.56 (+0.67%)	813.70 ± 9.34 (+0.91%)
28.8	789.34 ± 11.21 (+1.63%)	823.30 ± 11.73 (+2.10%)

Table 11: Wind Gust Impact on Energy

In this scenario it can be seen that the impact on energy consumption of both the consists is low even at high intensity wind gusts is low. It can be seen that in spite of gusts in favour and against the driving directions there is slight increase in energy consumption. This can be attributed to the quadratic nature of the resistance force caused by wind gust. It can also be seen that in this scenario the following train has slightly higher increase in energy consumption compared to the leading train. This shows that the gap controller requires higher control effort to maintain the gap between consists in comparison to the scenario where the headwind is constant.

Impact of Rolling resistance

From equation **(26)** we know rolling resistance has a linear relation in the resistance acting on the consists. A scenario with varying mean rolling resistance with zero standard deviation is simulated. From the results in Table 12 it can be seen that the energy consumption for both the leader and follower increases linearly with increasing rolling resistance.

Increase in Rolling Resistance (%)	Leader Energy (MWh)	Follower Energy (MWh)
1.0%	778.09 (+0.18%)	807.71 (+0.17%)
2.0%	779.47 (+0.36%)	809.07 (+0.34%)
5.0%	783.62 (+.89%)	813.16 (+0.84%)
10.0%	790.58 (+1.79%)	829.06 (+2.82%)

Table 12: Rolling Resistance Uncertainty Impact on Energy

Finally, a scenario with rolling resistance varying with different standard deviations with mean zero was simulated. The results in Table 13shows that due to the linear relationship to energy consumption there is no impact on the leader train. The follower train also has no significant impact showing that the gap control is able to compensate for the external disturbances with minimal control effort.

Rolling Resistance Standard Deviation (%)	Leader Energy (MWh) ± Std	Follower Energy (MWh) ±Std
1.0%	776.76 ± 0.20 (+0.01%)	806.95 ± 1.73 (+0.07%)
2.0%	776.57 ± 0.56 (-0.02%)	807.32 ± 2.61 (+0.12%)
5.0%	776.34 ± 0.97 (-0.05%)	806.80 ± 1.76 (+0.05%)
10.0%	777.09 ± 1.70 (+0.05%)	808.54 ± 2.50 (+0.27%)

Table 13: Rolling Resistance disturbance Impact on Energy

5.2.3 Tactical layer communication analysis

In an ideal world VCTS could enable consists to drive at RBD, since RBD is theoretically the distance required for consists to stop safely without collision. However, in the real world there is always a reaction delay (RD) due to uncertainties, delays and errors from various sources such as control errors, delay from power train and braking, uncertainties, errors and sampling rates of sensors and communication channels etc. To compensate for this an additional safety margin is to be considered in the minimum braking distance maintained with each other in a platoon.

The minimum safety margin that can be maintained in a platoon, depends on the cumulative RD. In case of VCTS since there are no mechanical links between trains and the gap between trains will be controlled via T2T communication. Therefore, for VCTS the reaction delay will be heavily influenced by the capabilities of communication channel between the trains and the relative sensors onboard. There are different possibilities for communication between trains. Communication can occur via T2G and G2T links or through direct T2T communication.

Today, T2G communication primarily relies on the GSM-R network. However, for virtual coupling, GSM-R may not provide the required performance. In the future, FRMCS will offer higher data rates, improved security, and low latency, which are crucial for T2T communication in a VCTS. This advanced communication technology will enable real-time transmission of absolute safe train positions (ASTP) and long range (LR) communication. A comparison of these technologies can be found in 3.4.2.3

The performance of ASTP and LRC may vary due to environmental factors such as terrains and obstacles or weather conditions. Furthermore, the communication technology available to different base stations along the railway networks maybe different. Therefore, each base station that enables the T2T communication will need to take the latency and probability of package drop outs into account to ensure safe VCTS operation.

In [124] different communication technologies and their performance are used to generate delay maps. These maps indicate the probability of different communication technologies to satisfy maximal delay for a given speed as a function of speed and distance. Such delay maps could be used to calculate safety margins required for different base stations that are responsible for VCTS.

For VCTS standalone applications since capacity improvement is not the priority, the relative distances can be higher than ABD and therefore, higher latencies can be acceptable. In this application the public networks (4G or 5G) may be used as T2T link for communication and ASTP and the SRC and RL onboard may be used to for ATP functionalities that VCTS may support.

Direct T2T communication is still an active area of research. In T48.4, different radio-based technologies for RL and SRC are evaluated. Direct T2T communication will provide even lower latency compared to T2G and G2T via FRMCS. This can be of critical importance, especially when virtually coupled trains are operating at short distances since, the operating distance can be in the order of tens of meters. Furthermore, this eliminates uncertainties arising from ASTP estimation. However, there are scenarios where SRC and RL alone may not be sufficient for VCTS.

For instance, during coupling and decoupling manoeuvre in VCTS, the train consists may be outside the range of onboard relative sensors. Additionally, track curvature may obstruct visibility between adjacent trains in the platoon. In T48.4, the capabilities of SRC and RL using radio-based technologies will be tested in real railway environments under various conditions. Similarly, there could also be scenarios where the LRC coverage and ASTP is limited or obstructed due to the environment for example while passing through a tunnel. In such scenarios the RL and SRC can provide the necessary T2T link for VCTS.

To ensure seamless coupling and decoupling, a long-range communication (LRC) link between trains is necessary. ASTP and T2G communication which enables long-range connectivity are essential for VCTS operation. To cover the full range of distances required for VCTS, a combination of RL, SRC, ASTP, and LRC is needed. This multi-layered approach enhances redundancy and reduces uncertainties, ensuring robust and reliable communication between virtually coupled trains for a wide range of scenarios. Thus, improving flexibility of the system and ability to adapt to environment and communication limitations.

6 CYBER SECURITY

6.1 INTRODUCTION

Recent events like the sabotage of more than 20 trains in Poland [125], which was carried out with a simple “radio-stop” command that could be broadcasted with easy to access equipment for ca. $30, highlight the importance of cybersecurity to protect modern railway systems. Cybersecurity attacks on rail companies in Belgium, China, Denmark, Germany, Russia, South Korea, Sweden, Switzerland, the UK and the US have been documented [126], which range from data breaches to critical disruptions. According to ENISA [127], ransomware attacks, data-related threats, and different forms of denial of service (DoS) attacks are the primary threats for the railway sector today. Especially the number of distributed DoS (DDoS) attacks as well as the sophistication of attacks in general has increased recently.

To tackle the situation, current and emerging EU regulations on cybersecurity such as the Cybersecurity Act, the Cybersecurity Resilience Act, and the NIS 2 Directive target increased resilience of our infrastructure. This is a key enabler for robust digitalization and automation, which in turn enable a better performing transport infrastructure through increased information sharing as, e.g., in VCTS. Adhering to these regulations is a challenge for all stakeholders within transport like infrastructure owners, manufacturers, operators, and service providers. It requires a deep integration of comprehensive cybersecurity frameworks into their systems and business. These frameworks must address risk assessment, data protection, and the continuous management of cybersecurity threats. It is no longer sufficient to treat cybersecurity as an afterthought, a more proactive approach is required that captures the evolving cybersecurity threat landscape as well as the interplay between safety and cybersecurity (i.e., cybersecurity threats that become safety risks and vice versa).

Within the following sections, we report a step towards a more proactive handling of cybersecurity issues by performing a cybersecurity risk assessment on the VCTS concepts presented in the previous chapters.

6.2 OBJECTIVE

Within Shift2Rail, a risk assessment process aligned with IEC 62443 has been developed and iteratively matured, to streamline the process for future projects of similar nature within the railway industry.

In the following, the risk assessment methodology, which largely follows the guidelines set up during the Shift2Rail project X2Rail-5 is introduced. Thereafter, a description of the system’s essential functions will be provided before the process is applied.

At the end of the process, the reader will receive risk and target security level evaluations for the system, a critical component for identifying applicable security requirements from IEC 62443.

To raise the quality of the assessment, experts from several project partners such as RISE, DLR, Renfe, Indra and CEIT were consulted. This included a physically held workshop in Gothenburg, Sweden.

6.3 Risk Analysis of VCTS

The IEC 62443 standard, which is used for industrial automation and control systems (IACS) has in earlier Shift2Rail projects been accepted as the main guideline for building cybersecurity robustness into railway systems. For example, as detailed in X2Rail-5 D11.1 [128], both X2Rail-1 and X2Rail-3 projects introduced simplified methodologies for risk assessment. However, following further enhancements, three comprehensive example assessments were presented in X2Rail-5 D11.1. Risk assessments were performed on both ATO GoA 2 and 3/4, as well as on the NG-TCN architecture designed by the Shift2Rail CONNECTA-3 working group. This iteration of the process is based on:

- IEC 62443 series [129] (esp., part "3-2 Security Risk Assessment for System Design").
- CLC/TS 50701 'Railway applications – Cybersecurity' [130].
- ISO 27000 series for conducting risk assessment (e.g., ISO 27001, ISO 27005).
- NIST special publications or IACS (e.g., NIST SP 800-82r2, NIST SP 800-39, NIST CSWPv1.1, NISTIR 8011, NIST SP 800-30r1).

Furthermore, threats are based on the Microsoft STRIDE threat model [131]. Likelihood is estimated using several factors, such as threat type, attacker's capability, intent and targeting, as well as assigned levels if Common Vulnerability Scoring System (CVSS) exploitability metrics [132]. For a more comprehensive description of this methodology than provided in this chapter, we refer to X2Rail-5 D11.1 [128].

Other initiatives have also developed methodologies for achieving the same purpose, such as EULYNX RCA OCORA which presented a risk assessment methodology in their '(Cyber) Security Guideline' document, accompanied by the 'ERORAT' (EULYNX RCA OCORA Risk Assessment Tool) Excel file [133].

X2Rail-5 D14.3 [134] compares these two different methodologies against IEC 62443, part 3-2 'Security risk Assessment for system design' and concluded that only X2Rail-5 D11.1 [128] is fully compliant with the standard (see Figure 58 below). Following this conclusion, the authors created a risk assessment tool according to the methodology in the form of an Excel file, which is now publicly available and provided together with the delivered report. The tool is intended to provide guidance for EU-Rail Innovation Pillar projects for the implementation of cybersecurity according to IEC 62443. Besides compliance with IEC 62443-3-2, the tool also covers the requirements of IEC 62443-3-3 and IEC 62443-4-2. As such, it will be utilised in this chapter for threat identification and risk assessment of VCTS within a limited scope. This means that while risk levels are assessed, the subsequent integration of mitigating measures is considered out of scope for this chapter. For a more comprehensive description of the tool, we refer to X2Rail-5 D14.3 [134].

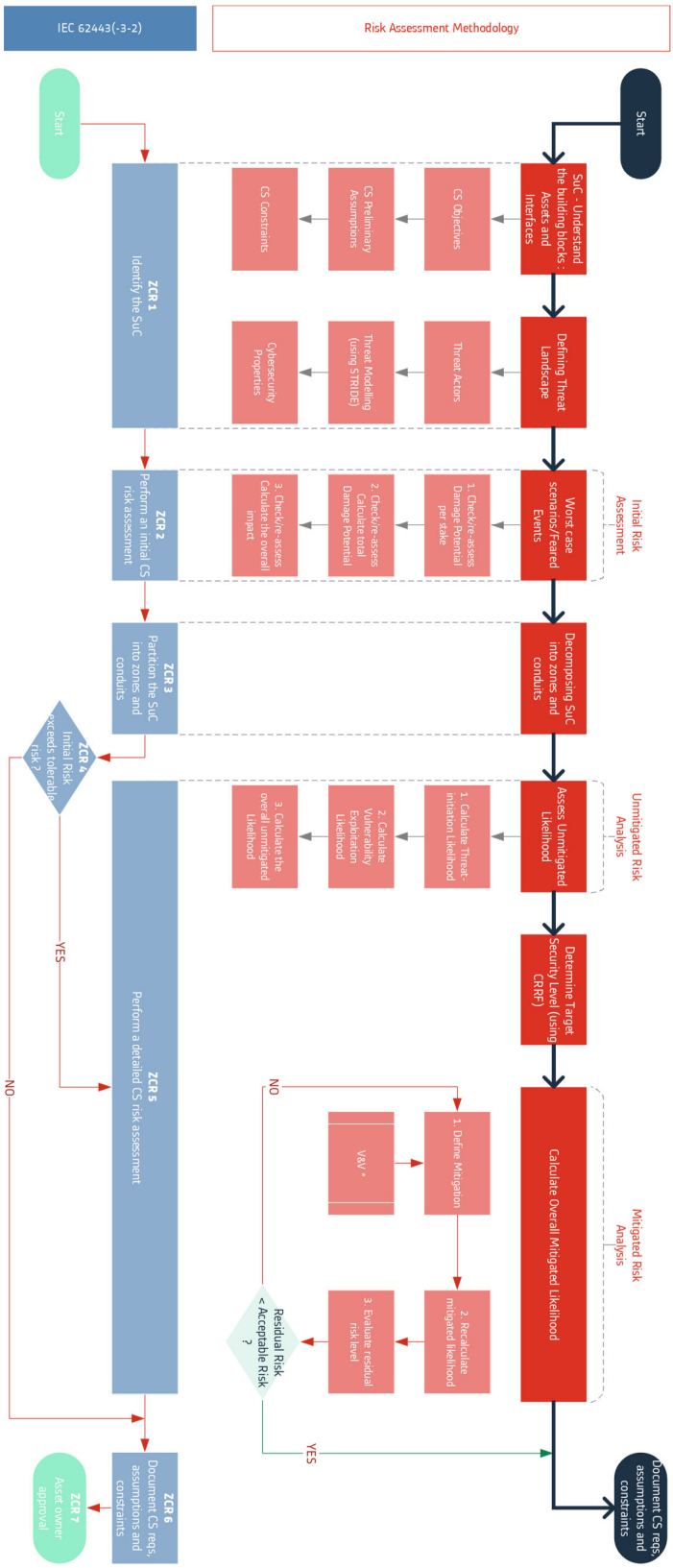

Figure 58: Risk assessment methodology flowchart **[134]**

6.3.1 VCTS – System Definition

6.3.1.1.1 System under Consideration (SuC)

Figure 29 displays a simplified block diagram derived from the technological baseline in Section 3.4, containing VCTS and its closest interacting components. It should be mentioned that this is a preliminary setup as the architecture might be subject to change in the future due to ongoing work on SRC. Also, it is still undecided whether VCTS-TS will communicate with VTCS-OB through TMS in the actual system design. It is possible to design a system with a direct logical interface through TCMS instead.

For this risk assessment, the scope of the system boundaries will be confined to the two VCTS components highlighted in green.

6.3.1.1.2 Security Zones and Conduits

IEC 62443 defines *security zones* as a “grouping of logical or physical assets that share common security requirements”. Zones can be either physical or virtual. In physical zones, assets are grouped based on their physical location, whereas in virtual zones the grouping is based on functionality or other characteristics.

Conduits are defined as a “logical grouping of communication assets that protects the security of the channel it contains”. They are a special type of security zone which logically groups information flows within or external to a zone.

Later, once risk levels have been assessed, requirements from IEC 62443-3-3 and IEC 62443-4-2 can be allocated to the zones and conduits. The zones and conduits identified for VCTS analysis are presented in Table 14.

Security Zones	
SZ-Name	SZ-ID
VCTS Onboard	OB-Z
VCTS Trackside	TS-Z

Table 14: VCTS security zones

The communication channels for VCTS is provided by the existing train network and other ETCS components like EuroRadio. As such, network and conduit components are considered out of scope for this risk assessment that specifically focuses on the VCTS system and its components.

6.3.1.1.3 Primary Assets

Several of the components in Figure 29 are together providing the nine operational scenarios of VCTS. These operational scenarios have been selected as the primary assets for this risk assessment during a physically held workshop with other project partners.

Primary assets are defined in CLC/TS 50701:2021 as the set of essential functions performed by the SuC to fulfil the system or subsystem’s objective(s). Hence, primary assets are comparable with how the term essential function is used in IEC 62443-3-3 as well.

Exactly which components are responsible for each scenario can be seen in Figure 59 below, taken from the Missions diagram of the VCTS Capella model introduced in the previous chapters. VCTS-OB has been excluded for visibility as it relates to all missions.

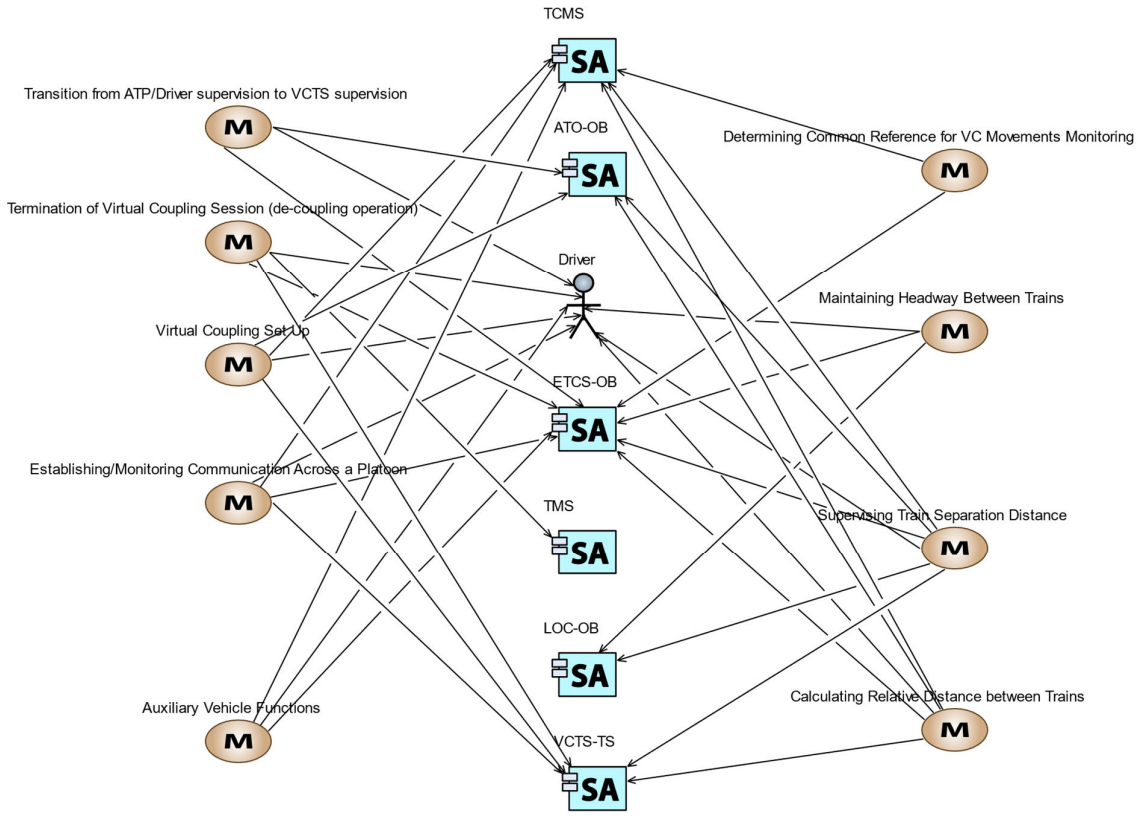

Figure 59: Missions diagram from VCTS Capella model (modified)

Brief summarising descriptions of each primary asset are provided in Table 15. For more detailed descriptions, we refer to the original source [24], where the operational scenarios of VCTS are described in detail.

Primary Assets	
Primary Asset ID	Description
F01 - Virtual Coupling Set Up	One of the trains initiates the virtual coupling procedure by opening a communication session with the other train candidate to form a platoon. Supervision moves from absolute to coordinated braking distance monitoring (see F02). The scenario assumes that at least the slave train includes some autonomous system that supports the driving according to the VCTS principles. Platoon may thereafter evolve to include more than one slave train. Refer: X2Rail-3 D6.1, Chapter 9.2

F02 - Transition from ATP/Driver supervision to VCTS supervision	The slave train is allowed to move closer to the master, beyond the limit imposed by the absolute braking distance. Supervision moves from absolute to coordinated braking distance monitoring. Refer: X2Rail-3 D6.1, Chapter 9.2
F03 - Supervision Train Separation Distance	Slaves monitor relative distance from Master train and from adjacent slaves. The relative distance takes into consideration safety factors due to difference in relative speed and acceleration, latency of the communication channel, positioning error, and different braking capabilities. Based on the exchanged information, slave train maintain safe distance from the rear end of the preceding trains, and eventually from the following train. Based on the continuous calculation, the slave train takes action to reduce speed or accelerate to adjust its position. Refer: X2Rail-3 D6.1, Chapter 9.3.1
F04 - Termination of Virtual coupling Session	Cooperative braking terminates only once the slave has reached a relative distance from master that is sufficient to cope with a 'full effort' braking action from the master. Once virtual coupling is terminated, the speed supervision mechanism of the split platoon becomes based on absolute braking distance. This means, the speed of the new created platoon shall slow down to cope with the new absolute braking distance supervision before considering the virtual coupling terminated. In case of radio connection loss, the slave train takes back autonomous control of its mission based on own data and supervision principles. If distance from preceding train is sufficient, according to absolute braking principles, no braking actions are required. Refer: X2Rail-3 D6.1, Chapter 9.4
F05 - Calculating Relative Distance Between Trains	Slave train follows the preceding train (master or slave) at safe distance, while also keeping a safe distance to the following slave. Speed and position may be subjected to accuracy uncertainties. Refer: X2Rail-3 D6.1, Chapter 9.7.1
F06 - Maintaining Headway Between Trains	Ensure, at all time, that the slave train does not breach the core safety principles, i.e.: it shall not, at any time, enter in collision with the master. The core of maintaining headway is the cooperative braking principle, that develops the concept of trains virtually coupled and braking as a single (virtual) platoon. The most relevant aspect is centred on the differences in terms of braking capabilities between trains within the platoon. Refer: X2Rail-3 D6.1, Chapter 9.7.2

F07 - Determining Common Reference for VC Movements Monitoring	If two trains shall monitor the relative distance for determining safety conditions under Virtual Coupling movements, this entails some algorithm to determine a common positioning reference system for both of them. The odometric system shall be considered as a source of data which is external to the VCTS and that provides input to the VCTS with adequate level of integrity and accuracy. Refer: X2Rail-3 D6.1, Chapter 9.7.4
F08 - Establishing/Monitoring Communication Across a Platoon	Cooperative Awareness Messages (CAMs) constitute a set of messages exchanged by mean of a protocol with the adequate level of safety and integrity, to allow master and slave consists to implement the necessary controls and supervision functions according to the Virtual Coupling concept. One of the key aspects of establishing a safe communication channel between virtually coupled trains is the possibility for the slave to distinguish the master to which to connect (or other way around). This analysis assumes the presence of a superior hierarchical entity that governs the coupling and determines which trains shall become part of a platoon. In case of temporary loss of wireless communication between one train and the rest of the platoon, a mechanism shall be provided inside VCTS functions to allow, once connection is re-established, that all other layers are still aligned, i.e.: the train composition is remained the same as before the communication loss, as well as the mission data like brake characteristics of any of the trains). Refer: X2Rail-3 D6.1, Chapter 9.7.6
F09 - Auxiliary Vehicle Functions	Master trains in a VCTS shall be allowed to drive a set of additional controls on the slave trains, as in standard multiple trains. - Pantograph management (raise/lower) - Doors control - Air tight control - Air conditioning activation/deactivation/adjust - Special brakes inhibition/activation (eddy current, magnetic shoe, regenerative, etc...) - Main switch open/close - Inhibit passenger's emergency brakes (in specific areas like tunnels, bridges, etc…) - Traction system configuration (1.5kV DC, 3kV DC, 25 kV AC, etc…) - CCTV - Passenger's information system - Boogie monitoring Refer: X2Rail-3 D6.1, Chapter 9.7.10

Table 15: VTCS primary assets

6.3.1.1.4 Supporting Assets

Supporting assets are components that the primary assets depend on to function. According to IEC 62443, supporting assets can be categorised into either embedded devices, network devices, software applications or host devices.

Supporting assets identified for VCTS analysis are presented in Table 16 below. As stated in [47], implementing virtual coupling functionality in the RCA and OCORA reference architectures would imply software implementation, laboratory and site testing activities without hardware impacts. Hence, VCTS is defined as a software application in the context of this chapter.

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

Table 16: VCTS Supporting Assets

6.3.1.1.5 System Definition Matrix

Which supporting asset(s) each primary asset is dependent upon can be extracted from the system definition matrix in

Table 17. As seen here, VCTS-OB is a required component for all primary assets.

VCTS-TS	VCTS-OB	Supporting Asset		Primary Asset
Software Applications	Software Applications	Supporting Asset Type		
X	X	VCSU		PA-01 Virtual Coupling Set Up
X	X	TAD-VS		PA-02 Transition from ATP/Driver supervision to VCTS supervision
X	X	STSD		PA-03 Supervision Train Separation Distance
	X	TVCS		PA-04 Termination of Virtual Coupling Session
X	X	CRDT		PA-05 Calculating Relative Distance between Trains
	X	MHBT		PA-06: Maintaining Headway Between Trains
	X	DCR-VMM		PA-07-PA-07 Determining Common Reference for VC Movements Monitoring
X	X	EM-CAP		PA-08 Establishing/Monitoring Communication Across a Platoon
	X	AVF		PA-09 Auxiliary Vehicle Functions

Table 17: System definition matrix

6.3.2 Initial Risk Assessment

The Initial Risk Assessment (IRA) in this methodology consist of evaluating impact from the perspective of confidentiality, integrity and availability, the so-called CIA Triad, on the following four business stakes (taken from X2Rail-5 D11.1 [128]):

- **Human safety:** Represents the impact in terms of health issues, injuries and human casualties of passengers, bystanders or personnel.
- **Performance:** Represents the impact in terms of disruption of the normal operation of the organisation and services.
- **Reputation:** This business stake is concerned with stakeholders' reaction and media coverage sheading a negative light on the organisation.
- **Compliance:** This business stake is concerned with conforming to regulations and contracts

This evaluation is performed for each primary asset. Each business stake can be impacted on one of four different levels of criticality, criteria for each being described in Table 18 below which corresponds to a certain damage potential (DP) value.

Level Description per Business Stake						
Impact Criticality Label	**Level**	**Damage Potential**	**Safety**	**Performance**	**Reputation**	**Compliance**
Critical	4	1000	Major loss of life (> 1).	All users experience prolonged and unplanned disruption to key routes. Access to major station facilities likely to be severely restricted. Major area blocked (e.g.: major city > 8H) or main infrastructure blocked during >1 week. If the fault occurs during use of the vehicles, then the vehicle must be decommissioned immediately (possibly trip to the next stop).	Extensive prolonged adverse national reporting (>1week) and public disputes with key stakeholders.	Extensive non-compliance to contracts, regulations and legislation with high penalties & liabilities (Personal liability with jail condemnation). Loss of license to operate.
Major<	3	100	Loss of 1 life, multiple major/severe injuries (> 20 injuries).	Unplanned disruption (for up to a week) on multiple routes (critical infrastructure). Major area blocked (e.g.: major city < 8H). If the fault occurs during use of the vehicles, then the vehicle can complete the current trip to strategically favourable place on the network (e.g. parking facility) or until a certain time.	Significant local/regional reports. National media interest during several days (< 1week) creating public concern. Negative national stakeholder statements.	Restriction to operate. Major non-compliance to contracts, regulations and legislation with penalties & liabilities (Personal liability with jail conditional condemnation).
Moderate	2	10	No loss of life, Multiple minor injuries, one or multiple major	Unplanned disruption (for up to a week) on any one route or Up to a day on multiple routes. No impact on most critical infrastructure. Train replacement at the end of the	Adverse local/regional media reports over a period. Localised	Medium non-compliance to contracts, regulations and legislation with Low penalties &

			injuries (< 20 injuries).	trip (train back empty to depot).	stakeholder concern.	liabilities. (Personal liability with financial condemnation).
Minor	1	1	No loss of life, minor injuries.	Unplanned disruption (for up to a day) on one route or No service delays. Non-scheduled maintenance operation to be performed in the worst case. (max. seven calendar days)	Adverse local stakeholder reaction.	Minor non-compliance to contracts, regulations and legislation with Low penalties & liabilities.

Table 18: Criticality Labels for different Business Stakes

The sum of all damage potential is thereafter mapped to an overall impact rating using Table 19 below.

Impact Severity	Total (DP) value
1	4 - 30
2	31 - 220
3	221 - 400
4	Equal or greater than 401

Table 19: Impact severity tier list

The evaluation of impact was performed in pairs, with experts from several project partners such as RISE, DLR, Renfe, Indra and CEIT. Each primary asset has been independently evaluated by two separate pairs, whereafter the principle of worst case was applied to determine the final impact on each business stake. Meaning that the higher level of impact was always chosen as final. In total, 12 cybersecurity and subject matter experts participated in this activity of initial cybersecurity risk assessment. The results of this exercise can be seen in Table 20 to Table 22 below.

Feared-Events	Security-Criteria	Safety	Performance	Reputation	Compliance	DPTotal	Overall Impact	Rationale per security criteria
Loss of Confidentiality FE-01 Virtual Coupling Set Up	Confidentiality	1	1	2	3	112	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Integrity FE-01 Virtual Coupling Set Up	Integrity	3	4	3	3	1300	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-01 Virtual Coupling Set Up	Availability	4	3	2	3	1210	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Confidentialiaty FE-02 Transition from ATP/Driver supervision to VCTS supervision	Confidentiality	1	1	2	2	22	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Integrity FE-02 Transition from ATP/Driver supervision to VCTS supervision	Integrity	4	4	4	3	3100	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-02 Transition from ATP/Driver supervision to VCTS supervision	Availability	1	3	2	2	121	3	Safety: Loss of 1 life, multiple injuries >20 Performance: Train cannot finish the trip. Block route Reputation: Significant local/regional media reports and national media reports during several days Compliance: Major non-compliance to contract
Loss of Confidentiality FE-03 Supervision Train Separation Distance	Confidentiality	4	4	3	3	2200	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Integrity FE-03 Supervision Train Separation Distance	Integrity	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-03 Supervision Train Separation Distance	Availability	4	4	3	3	2200	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Confidentiality FE-04 Termination of Virtual Coupling Session	Confidentiality	1	1	2	1	13	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Integrity FE-04 Termination of Virtual Coupling Session	Integrity	4	4	3	3	2200	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract

Table 20: VCTS Initial Risk Assessment (1/3)

Loss of Availability FE-04 Termination of Virtual Coupling Session	Availability	1	2	2	1	22	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Confidentiality FE-05 Calculating Relative Distance between Trains	Confidentiality	1	1	2	2	22	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Integrity FE-05 Calculating Relative Distance between Trains	Integrity	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-05 Calculating Relative Distance between Trains	Availability	1	2	2	2	31	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation
Loss of Confidentiality FE-06 Maintaining Headway Between Trains	Confidentiality	4	4	3	4	3100	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Integrity FE-06 Maintaining Headway Between Trains	Integrity	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-06 Maintaining Headway Between Trains	Availability	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Confidentiality FE-07 Determining Common Reference for VC Movements Monitoring	Confidentiality	1	1	1	3	103	1	Safety: No loss of life, no injure Performance: No disruption Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract
Loss of Integrity FE-07 Determining Common Reference for VC Movements Monitoring	Integrity	4	3	2	3	1210	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-07 Determining Common Reference for VC Movements Monitoring	Availability	4	4	3	3	2200	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Confidentiality FE-08 Establishing/Monitoring Communication Across a Platoon	Confidentiality	1	1	2	2	22	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation

Table 21: VCTS Initial Risk Assessment (2/3)

Loss of Integrity FE-08 Establishing/Monitoring Communication Across a Platoon	Integrity	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-08 Establishing/Monitoring Communication Across a Platoon	Availability	4	2	4	3	2110	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Confidentiality FE-09 Auxiliary Vehicle Functions	Confidentiality	1	2	3	2	121	3	Safety: Loss of 1 life, multiple injuries >20 Performance: Train cannot finish the trip. Block route Reputation: Significant local/regional media reports and national media reports during several days Compliance: Major non-compliance to contract
Loss of Integrity FE-09 Auxiliary Vehicle Functions	Integrity	4	4	4	4	4000	4	Safety: Major loss of life Performance: Major area blocked or main infrastructure blocked during >1week Reputation: Extensive national media reports Compliance: Extensive non-compliance to contract
Loss of Availability FE-09 Auxiliary Vehicle Functions	Availability	1	2	2	3	121	2	Safety: No loss of life, no injure. Performance: Train might need to be replaced after the trip Reputation: Adverse local/regional media reports Compliance: Major non-compliance to contract and regulation

Table 22: VCTS Initial Risk Assessment (3/3)

6.3.3 Unmitigated Risk Analysis

The initial risk assessment is followed by a more detailed, so-called “unmitigated risk analysis” (as mitigations have not been implemented yet). While the former focused on the assessment of impact, the unmitigated risk analysis proceeds by evaluating the “likelihood” parameter. Once this has been assessed as well, impact and likelihood are multiplied to form the definitive risk levels.

6.3.3.1 Event Initiation Likelihood

Inherited from the Shift2Rail CONNECTA-3 working group, the methodology in X2Rail-5 D11.1 [128] examines nine types of threat actors capable of triggering threats in the railway domain: Hacker/Cracker, Terrorist, Competitor, Government Organisation, Hacktivist, Criminal Organisation, Script Kiddy, Layman and Insider. These actors are characterised by different levels of “Capability”, “Intent” and “Targeting”. Descriptions of these likelihood criteria has for completeness been repeated in Table 23 below.

	Unlikely (1)	**Possible (2)**	**Likely (3)**	**Certain (4)**
Capability	The attacker has limited resources, expertise, and opportunities to support a successful attack.	The attacker has moderate resources, expertise and opportunities to support multiple successful attacks.	The attacker has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.	The attacker has a very sophisticated level of expertise, is well-resourced and can generate opportunities to support multiple successful,

	Unlikely (1)	Possible (2)	Likely (3)	Certain (4)
				continuous and coordinated attacks.
Intent	The attacker actively seeks: - to obtain critical or sensitive information. - to disrupt the system's cyber resources. The attacker does not concern about attack detection or disclosure.	The attacker seeks: - to obtain or modify specific critical or sensitive information; - to disrupt the system's cyber resources; - to impede system functionalities by establishing a foothold in the organization's IS/ICS. The attacker is concerned about minimizing attack detection/disclosure, particularly when carrying out attacks over long time periods.	The attacker seeks: - to undermine or impede critical aspects of a core system function; - to place itself in a position to do so in the future by maintaining a presence in the system. The attacker is very concerned about minimizing attack detection/disclosure, particularly while preparing for future attacks.	The attacker seeks: - to undermine, severely impede, or destroy a core business function or component by exploiting a presence in the system. The attacker is concerned about disclosure only to the extent that it would impede its ability to complete stated goals.
Targeting	The attacker uses publicly available information: to target a class of high-value railway vendors / companies / organizations. by seeking: - targets of opportunity of this class.	The attacker analyses publicly available information: to target persistently specific high-value railway vendors / companies / organizations. by focusing on: - key position employees; - programs; - the system itself; - information used by the system.	The attacker analyses information obtained via reconnaissance: to target persistently a specific organization, enterprise, railway system or system function. by focusing on: - specific high value or mission critical information; - resources; - supply flows; - system functions or specific employees supporting these functions; - key position employees.	The attacker analyses information obtained via reconnaissance and attacks: to target persistently a specific organization, enterprise, railway system or system function. by focusing on: - specific high value or mission critical information; - resources; - supply flows; - system functions, or specific employees supporting these functions or even supporting infrastructure: - key position employees; - providers / suppliers;

	Unlikely (1)	Possible (2)	Likely (3)	Certain (4)
				- partner organizations.

Table 23: Likelihood criteria descriptions

We have reassessed these likelihood criteria for each threat actor with regards to the current system under consideration (VCTS), again in consultation with project partners. The results from this exercise can be seen in Table 24 below. There are some noteworthy differences compared to the results for Automatic Train Operation (ATO) Grade of Automation (GoA) 3/4 presented in X2Rail-5 D11.1 [128]:

- "Competitors" were considered to possess higher capability, while intent and targeting were simultaneously lowered. One motivation for this is that while competitors in this sector may possess extensive knowledge, it is unlikely that they would attack each other.
- Increased intent for "Terrorist". A motivation for this is that they likely possess a high motivation to enforce their ideological beliefs.
- Increased targeting for "Government Organisation". 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.

Threat Actor	Capability	Intent	Targeting
Hacker / Cracker	3	3	3
Terrorist	3	4	4
Competitor	4	3	2
Government Organisation	4	3	3
Hacktivist	3	3	3
Criminal Organisation	4	4	4
Script Kiddy	2	2	2
Layman	1	1	2
Insider	4	3	4

Table 24: VCTS Likelihood criteria evaluations

Together with assigned weights, the Excel tool utilises the capability, intent and targeting values to calculate an "Event Initiation Likelihood" (EIL) value for each threat actor. In this assessment the default weights were kept, and we refer to X2Rail-5 D11.1 [128] for a description of the underlying formulas.

The resulting event initiation likelihood for each threat actor is presented in Table 25 below, which are averaged to form the so-called balanced EIL.

Weights/Multiplicative Factor			Consideration factor of threat actor (if an actor is not relevant please use "0" for the specifc threat actor)									
CAP	INT	TARG	1	1	1	1	1	1	1	1	1	1
1	2	3	Event Initiation Likelihood (EIL)									
			Hacker/Cracker	Terrorist	Competitor	Government Organization	Hacktivist	Crimical Organization	Script Kiddy	Layman	Insider	Max 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 25: VCTS Event Initiation Likelihood

The pessimistic EIL, which is the balanced rounded up, will represent the whole system going forward.

6.3.3.2 Threat Landscape

The first version of a X2Rail-developed risk assessment methodology, presented in X2Rail-1, applied a general threat landscape [128]. The Shift2Rail X2Rail project realised that a threat landscape tailored towards the current and emerging trends within railway cybersecurity is required. This need was fulfilled through the integration of MITRE attack techniques: https://attack.mitre.org/techniques/ics/

Table 36: Threat **Landscape** X2Rail-5 D11.1 [128] presents the threat landscape with a list of potential threats which could menace the environment if its vulnerabilities are exploited. The threats are grouped according to the Microsoft STRIDE threat model domains as described by X2Rail-3 D8.1:

Threat	Desired Property	Description
Spoofing	Authenticity	**Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's or entity authentication information, such as username and password. **Spoof** - pretend to be an authorized user and perform an unauthorized action.
Tampering	Integrity	**Tampering with data**. Tampering with SW, HW and data - Infection with malicious software or hardware could lead to malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two entities over an open network, such as the Internet.
Repudiation	Non-repudiability	**Repudiation**. Repudiation threats are associated with users or entities who deny performing an action without other parties having any way to prove otherwise—for example, a user or entity performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for

Threat	Desired Property	Description
		the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package. Repudiation - denial by one of the entities involved in a communication of having participated in all or part of the communication.
Information Disclosure	Confidentiality	**Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users or entities to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two machines.
Denial of Service	Availability	**Denial of service**. Denial of service (DoS) attacks deny service to valid users or entities —for example, by making a Web server or RBC temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability. **Denial of service** - prevention or interruption of authorized access to a system resource of the delaying of system operations and functions.
Elevation of Privilege	Authorisation	**Elevation of privilege**. In this type of threat, an unprivileged user or unauthorized entity gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself, a dangerous situation indeed.

Table 26: Microsoft STRIDE Threat Model domains

The inclusion of STRIDE threat modelling technique was initially made by X2Rail-3 D8.1 [135]. Table 25 in X2Rail-5 [128] builds upon this by mapping STRIDE domains to the CIA-properties Confidentiality, Integrity and Availability commonly encountered within the cybersecurity field. It also allocates threats according to the supporting asset types defined in IEC 62443: Software Applications, Network Devices, Host Devices and Embedded Devices.

6.3.3.3 Unmitigated Likelihood

In this part of the assessment, a vulnerability rationale and CVSS score is derived for each supporting asset. The inclusion of CVSS scoring system v3.1 for risk assessment was motivated in [135] by being simple enough to cover the required detail while not hiding the result behind a lot of formulas and variables.

The vulnerability rationale used to derive the CVSS vector is inherited from X2Rail-5 D11.1 [128] and repurposed for this report. However, it should be mentioned that these could be made obsolete in the future due to ongoing work on short-range communication for VCTS. For the context of this chapter, it is assumed TCMS handles this type of communication.

The CVSS vector outputs a score which is further normalised using Table 27 below and thereafter referred to as “Unmitigated Vulnerability Severity (UVS)”. The term “unmitigated” signifies that the parameter is evaluated before applying any risk reducing measures to the system.

Unmitigated Vulnerability Severity	(unmitigated) CVSS Score
1	0 ≤ UCVSS < 4
2	4 ≤ UCVSS < 7
3	7 ≤ UCVSS < 9
4	9 ≤ UCVSS ≤ 10

Table 27: Unmitigated Vulnerability Severity

Furthermore, the UVS outputs can be consolidated with the EIL result from Section 6.3.3.1 into an "overall unmitigated likelihood" through the following formula:

$$\text{Overall Unmitigated Likelihood} = \left\lfloor \frac{UVS \times EIL}{4} \right\rceil$$

where "⌊ ⌉" represents rounding to nearest integer.

The overall unmitigated likelihood is calculated for each supporting asset and STRIDE domain, results presented in Table 28 below:

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	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.5	2	3	1

SA-ID	STRIDE Threat Category	Vulnerability Rationale	CVSS Vector	CVSS Score	UVS	EIL	Overall Unmitigated Likelihood
		+ remote access interface (e.g. SSH)					
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
VCTS-TS	Spoofing Identity	Attacker can access VCTS-TS 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-TS	Tampering with data	Attacker can access VCTS-TS 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-TS	Repudiation	Attacker can access VCTS-TS 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-TS	Information disclosure	Attacker can access VCTS-TS 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-TS	Denial of Service	Attacker can perform DoS attack via ETCS or TCMS network	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.5	2	3	1
VCTS-TS	Elevation of Privilege	Attacker can access the VCTS-TS 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 28: VCTS Overall Unmitigated Likelihood

6.3.3.4 Unmitigated Risk

Below, Table 29 analyses the threat influence of each supporting asset on their corresponding primary assets (only results for primary asset 1 presented here, full table provided in Appendix B, Table 26-32). The unmitigated risk is calculated here by multiplying impact with likelihood, which is a critical parameter for determining target security level (SL-T) and later allocating security requirements from IEC 62443. MITRE threats have also been identified for each supporting asset, in accordance with the threat landscape described in Section 6.3.3.2.

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] See Table 26-32 for detailed attack techniques	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] See Table 26-32 for detailed attack techniques	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Information Disclosure	[DISCLOSING INFORMATION FROM SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Confidentiality	2	1	2
PA-01 Virtual Coupling Set Up	VCTS-OB	Denial of Service	[DoS Software Applications] See Table 26-32 for detailed attack techniques	Availability	4	1	4
PA-01 Virtual Coupling Set Up	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Confidentiality	2	2	4
PA-01 Virtual Coupling Set Up	VCTS-TS	Spoofing Identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] See Table 26-32 for detailed attack techniques	Integrity	4	2	8

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-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-TS	Information Disclosure	[DISCLOSING INFORMATION FROM SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Confidentiality	2	1	2
PA-01 Virtual Coupling Set Up	VCTS-TS	Denial of Service	[DoS Software Applications] See Table 26-32 for detailed attack techniques	Availability	4	1	4
PA-01 Virtual Coupling Set Up	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] See Table 26-32 for detailed attack techniques	Confidentiality	2	2	4

Table 29: VCTS Unmitigated Risk

Figure 60 below analyses the maximum level of unmitigated risk per primary asset, sorted by the CIA-properties Confidentiality, Integrity and Availability.

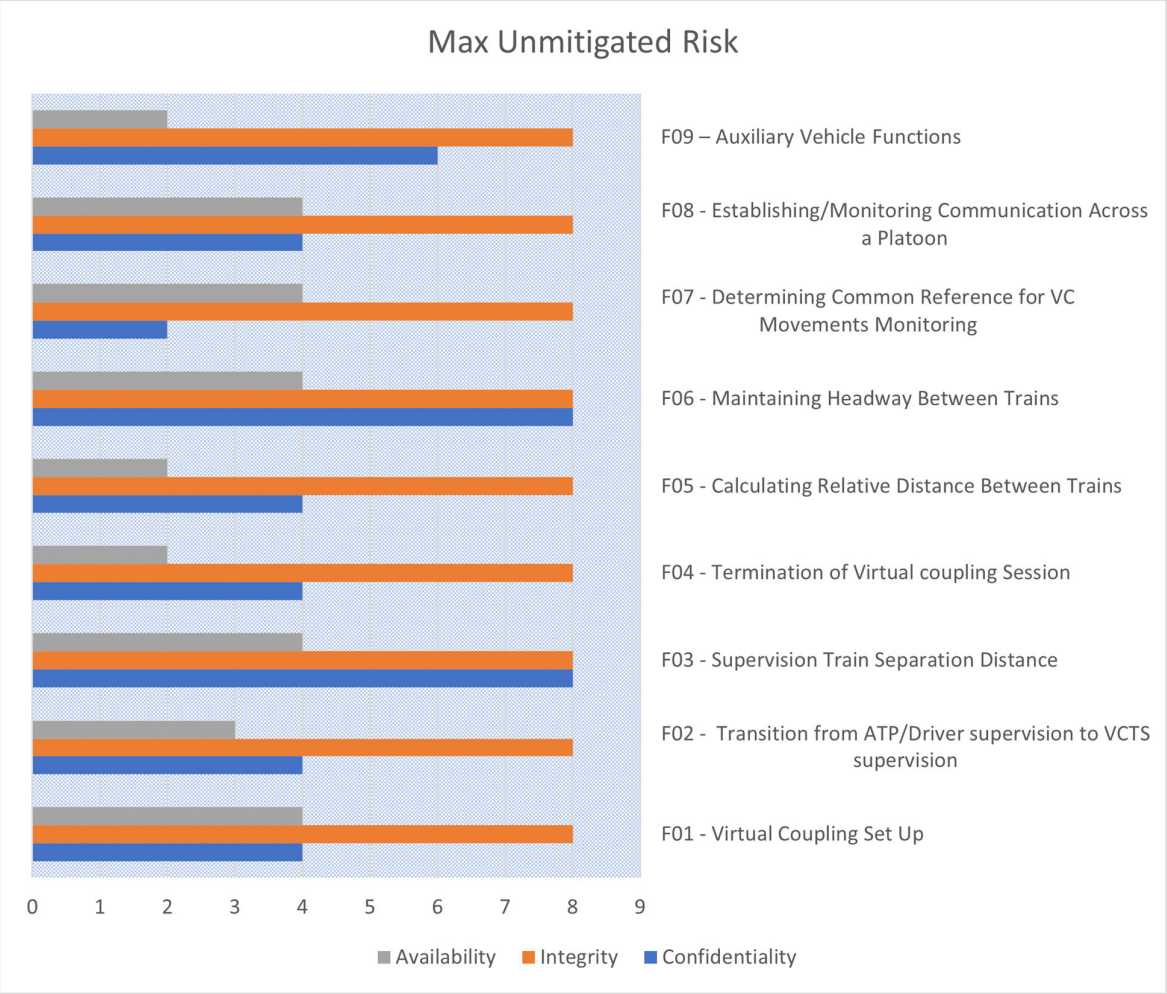

Figure 60: Max Unmitigated Risk (CIA)

Table 30 presents the maximum unmitigated risk, sorted by STRIDE domain (see Table 26) and security zone.

Max Risk per Zone	Spoofing Identity	Tampering with data	Repudiation	Information Disclosure	Denial of Service	Elevation of privilege
OB-Z	**8**	**8**	**8**	**4**	**4**	**8**
TS-Z	**8**	**8**	**8**	**4**	**4**	**8**

Table 30: Risk per Zone

In Table 31, the same risk levels are mapped to their corresponding target security level (SL-T), meaning the security level (SL) which the system needs to achieve:

Tolerable Risk = 4	
Unmitigated Risk	**SL-T**
1	0
2	0
3	0
4	1
6	2
8	2
9	2
12	3
16	4

Table 31: Risk vs SL-T

Furthermore, IEC 62443-3-3 provides the following definitions of security level 1 to 4 (no specific requirements or security protection necessary for SL 0):

- SL 1: Protection against casual or coincidental violation.
- SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation.
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

Max SL-T per Zone	**S**poofing Identity	**T**ampering with data	**R**epudiation	**I**nformation Disclosure	**D**enial of Service	**E**levation of Privilege
OB-Z	**2**	**2**	**2**	**1**	**1**	**2**
TS-Z	**2**	**2**	**2**	**1**	**1**	**2**

Table 32: SL-T per Zone and STRIDE domain

The STRIDE domains can hereafter be mapped to the seven foundational requirements (FR) of IEC 62443 for identifying appropriate requirements to achieve a specific target security level (SL-T):

- FR 1: Identification and authentication control (IAC)
- FR 2: Use control (UC)
- FR 3: System integrity (SI)
- FR 4: Data Confidentiality (DC)
- FR 5: Restricted data flow (RDF)

- FR 6: Timely response to events (TRE)
- FR 7: Resource availability (RA)

Table 33 maps target security levels to the foundational requirements, whereafter the highest for each is used going forward, as described in X2Rail-5 D11.1 [128].

SL-T-FR	Calculation formula
IAC	Max(SL-T**S**, SL-T**R**, SL-T**E**)
UC	Max(SL-T**S**, SL-T**R**, SL-T**E**)
SI	Max(SL-T**T**)
DC	Max(SL-T**I**, SL-T**E**)
RDF	Max(SL-T**S**, SL-T**I**, SL-T**D**)
TRE	Max(SL-T**S**, SL-T**T**, SL-T**R**, SL-T**I**, SL-T**D**, SL-T**E**)
RA	Max(SL-T**D**)

Table 33: STRIDE vs. IEC 62443 FR

Resulting from this risk assessment, the SL-T vector is presented in Table 34 below.

	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 34: SL-T per Zone and IEC 62443 FR

While the definition of these SL has been provided in earlier in this section, Table 7 in X2Rail-5 D11.1 [128] provides further rationale description for their implications:

- SL 1: “the Likelihood and the Impact are low: in this case, the risk level is equal to the Tolerable (Acceptable) risk level: we accept that we are protected against casual or coincidental (thus non-intentional) attacks. Protection measures implemented are of the lowest Security Level (SL1)”
- SL 2: “the average of the Likelihood and the Impact is 2 (medium) while none of the two factors (either the Likelihood or the Impact) is very low. Advanced security measures shall be implemented compared to those in SL1, to ensure the protection against intentional attacks of medium severity.”

Using the SL-T vector, organisations can identify and allocate requirements from IEC 62443-3-3 (for zone/system level) as well as IEC 62443-4-2 (for component/supporting asset level) to address potential cybersecurity risks. As an example, the Foundational Requirements (FR) for Data Confidentiality (DC) from IEC 62443-3-3 are provided in Table 35, along with indication to which of them that need to be fulfilled in order to achieve a particular target security levels (SL-T). A comprehensive mapping for all FRs and component requirements is not included at this stage, as the VCTS reference architecture is not yet formalized and the current assessment is based on RCA and OCORA assumptions, where VCTS-OB and VCTS-TS are treated as software components; this

classification may change to an embedded or host-based device in later design phases, impacting the applicable requirement set. Nevertheless, the same methodology for deriving and allocating IEC 62443 requirements from the SL-T vectors would apply, independently of the final architectural realization of the VCTS.

FR 5 — Data confidentiality (DC)	SL 1	SL 2	SL 3	SL 4
SR 4.1 — Information confidentiality	✓	✓	✓	✓
SR 4.1 RE 1 — Protection of confidentiality at rest or in transit via untrusted networks		✓	✓	✓
SR 4.1 RE 2 — Protection of confidentiality across zone boundaries				✓
SR 4.2 — Information persistence		✓	✓	✓
SR 4.2 RE 1 — Purging of shared memory resources			✓	✓
SR 4.3 — Use of cryptography	✓	✓	✓	✓

Table 35: Zone/system level Data Confidentiality (DC) FR from IEC 62443-3-3

6.3.4 Comparison to ATO risk assessment of X2Rail-5

Compared to the assessments performed in X2Rail-5 D11.1 [128] the resulting SL-T vector looks very similar to that of ATO GoA 2, with the only difference being a one level higher SL-T for FR requirement “DC”. Just like in our case, ATO GoA 2 SuC was divided into an on-board and track-side zone.

ATO GoA 3/4 however consisted of five security zones, three of which received SL-T 3 for certain FR. One explanation for this is that our experts evaluated the (pessimistic) event initiation likelihood (EIL) to three instead of four, resulting in the calculations for overall unmitigated likelihood to not surpass the value two. This in turn capped the maximum risk level to eight.

ATO GoA 2 also received an EIL value of four, however in that case the overall impact levels remained lower, only between 1-2 after the initial risk assessment. It is difficult to pinpoint exactly why the evaluation would differ for each parameter between these assessments. Cybersecurity risk assessments are lengthy processes, relying heavily on the expertise of the assessors and the outcome of discussions among them. Another aspect that likely contributed to different viewpoints between VCTS and ATO is the definition of VCTS as a software application, instead of an embedded or host device.

6.4 Conclusion

This chapter presented a risk assessment of VCTS following the methodology presented in X2RAIL-5 D11.1 [128] and using the complementing Excel tool made publicly available by X2RAIL-5 D14.3 [134]. These deliverables are a significant step forward towards increasing IEC 62443 compliance within the railway industry. The tools and the methods produced in these deliverables are sufficiently developed and mature so that an assessor isolated from its development is able to utilise them. To the best of our knowledge, no prior impact or risk assessment aligned with both with the IEC 62443 series and TS 50701 has been presented for VCTS.

In this assessment, VCTS consists of two security zones (OB-Z and TS-Z) with resulting target security level (SL-T) for six of seven of IEC 62443's foundational requirements being 2 and one (RA, resource availability) being 1, as detailed in Table 34. In the context of this deliverable, a list of recommended security requirements has not been provided since focus has mainly been on evaluating the unmitigated risk levels. However, these can be extracted from IEC 62443 using the given SL-T vector, as explained in Section 6.3.3.4.

VCTS is a complex concept and is still evolving at the time of this writing. Parts of its architecture might be subject to change. As seen in the Figure 29, VCTS interacts and depends on many other components of the railway system that were left out of the system under consideration to preserve a manageable scope for the context of this project. Finally, while this thorough analysis achieved its goal of assessing risk levels for VCTS, it would be of large interest to in the future increase the scope by also encompassing related parts of surrounding systems (for example as additional zones), paving the way for modern and robust operational solutions.

6.5 Future Work

This work has generated several insights into how we believe the methodology could be further improved during future projects. Most prominently, we believe that the vulnerability severity analysis, which is part of the unmitigated risk analysis can be expanded to better guide users into creating more precise vulnerability vectors using CVSS. As mentioned in Section 6.3.3.3, the vulnerability rationales used in this chapter were inherited and repurposed from X2Rail-5 D11.1 [128]. We believe that more specific rationales would further help in guiding the following development process including mitigations. Unifying existing approaches like attack trees mentioned in [128] into the methodology more effectively could improve the vulnerability severity analysis. We argue that this would greatly increase the applicability of this methodology to other railway systems as well.

As an example, X2Rail-5 D11.1 [128] also presents a risk assessment of Next Generation Train Control Network (NG-TCN), where attack trees are utilised for likelihood estimation. However, this approach deviates from the ATO GoA 2 and 3/4 assessments and readers are not provided with an insight into the process of creating them. Such examples, as well as guidelines for utilising attack trees harmonised within the methodology itself would be of major aid for creating more precisely tailored vulnerability rationales and CVSS vectors. The authors themselves mention that the whole methodology was modified for this case only, including threat landscape, likelihood assessment and impact evaluation.

Another resource we believe could be utilised for improving the vulnerability severity analysis are the MITRE attack techniques. As seen in the Threat Landscape (Table 36: Threat Landscape), these vulnerabilities have been categorised into the STRIDE domains and allocated to different IEC 62443 supporting asset types. However, besides providing a list of threats applicable to the SuC, the methodology does not fully guide users yet on how this information can improve risk assessment results, more specifically the likelihood estimation.

It can further be mentioned that the current risk assessment method focuses on IEC 62443-3-2 and technical measures, but not the critical role of people, processes, and services in cybersecurity. The method also mainly addresses primary functions, omitting the vital inclusion of information assets, which are essential for risk analysis and management outside the System under Consideration (SuC). To align with ISO 27001 standards, the methodology should integrate the classification and management of information assets to further ensure comprehensive risk management.

Lastly, it would greatly increase the legitimacy of the threat landscape presented by X2Rail-5 D11.1 [128] should it be aligned with the Transport Threat Landscape for the European Union, made by the European Union Agency for Cybersecurity (ENISA) [127].

As the Baseline 1 of the System Pillar documentation has been published after the initial finalisation of this Deliverable one specific further activity has to be a detailed comparison of the approach presented here with the specification documents of this baseline similar to the one made with OCORA.

Furthermore, is to be remarked that many of the today's systems as e.g. current interlockings in use are specified, developed and certified to an absolute braking distance principle. The relative braking distance principle used here still needs to be analysed and certified to fulfil all the technical and procedural requirements.

7 CONCLUSIONS

Deliverable D48.2 built upon the Virtual Coupling Train System (VCTS) concept developed in previous projects, notably CONNECTA-2 and X2Rail-3, and extended its definition within Europe's Rail framework. The primary objectives were to define the VCTS concept, identify use cases, establish system design and interfacing based on state-of-the-art technologies, propose VCTS driving strategies, and assess cybersecurity risks.

A comprehensive review of relevant projects from 2018 to 2023, including Connecta-1,2,3, X2Rail-3, SCOTT, MovingRail, and INSECTT, provided an overview of key research topics, developments, and challenges associated with VCTS. Four primary use cases were identified: mainline freight, mainline passenger, low-density networks, and urban mass transit. Each presented unique operational characteristics and stakeholder interactions, offering valuable insights for future deployment strategies.

A technological baseline for VCTS was also established, demonstrating its alignment with the most consolidated reference architectures available at the time of drafting this deliverable, including RCA for trackside systems and OCORA for onboard systems. Key enabling technologies such as localization and communication systems were examined, highlighting the shift towards onboard systems and reducing trackside dependencies—a significant paradigm change in railway operations. The analysis also emphasized the necessity of the Future Railway Mobile Communication System (FRMCS) for VCTS implementation, while legacy systems like Eurobalises and GSM-R remained relevant for degraded operational scenarios, offering valuable insights for future stakeholder alignment.

The deliverable reviewed literature on various map-supported localization technologies and underscored the importance of onboard localization units comprising GNSS, IMU, and velocity sensors. A more flexible approach to integrating new sensor technologies and accessing data was identified as essential for maximizing VCTS performance. Further empirical validation through data collection and software simulations was recommended on this front. Communication architectures were analyzed, referencing the current IEC 61375 Train Communication Network (TCN) and its potential migration to the Next Generation TCN (NG-TCN) proposed by the System Pillar. A model-based systems engineering (MBSE) approach was applied to analyse interfaces and data streams, providing insights into communication requirements for VCTS manoeuvre.

The deliverable also detailed the operational concept of VCTS, the layered decision framework, and the information flow required for platoon coordination. It demonstrated how the tactical layer can orchestrate train coupling and decoupling under different operational requirements. Various use case examples illustrated how the tactical layer coordinated manoeuvre to meet schedules, minimize energy consumption, and maximize capacity. Furthermore, dynamic simulations of VCTS operations were analyzed, assessing train interactions within a VCTS platoon. The results demonstrated bidirectional train coupling and decoupling based on operational focus and scenario, highlighting that VCTS performance ultimately depended on scenario-specific constraints such as speed limits, train-to-train communication rates, and railway switch speeds.

A risk assessment was conducted using methodologies from X2Rail-5, ensuring compliance with IEC 62443 and TS 50701 standards. VCTS was analyzed within two security zones (OB-Z and TS-Z), with foundational security levels assessed for potential vulnerabilities. While unmitigated risks were successfully evaluated, further work was deemed necessary to define specific security

requirements and extend the scope to additional railway components, providing valuable insights for stakeholders interacting with VCTS unit.

Several challenges emerged, including the need for standardized architectures to accommodate rapid technological advancements and the complexity of integrating VCTS with existing and future signalling systems. Since the completion of the deliverable tasks, SP has released Traffic CS and a Train CS architecture baseline as part of efforts unify EU-level visions for future railway system architecture. To ensure VCTS technological developments remain aligned with ongoing work in SP a detailed analysis of the differences between selected OCORA and RCA architectural baselines and SP CS architecture will be necessary in the future.

Future efforts should also focus on increasing data collection and software simulations to refine localization and control algorithms, exploring the integration of advanced communication and sensor technologies, including those from Task 48.4, and expanding risk assessments to encompass broader railway system interactions and cybersecurity considerations. Further assessments of attainable performance, refinement of interfaces, and alignment with emerging railway technologies and architectures are also recommended.

Deliverable D48.2 made a significant contribution to advancing the VCTS concept within Europe's Rail framework. By addressing system design, operational strategies, and cybersecurity aspects, it lays a solid foundation for future developments in virtual coupling and its potential to transform railway operations.

APPENDIX A

Security property	Threat Category	Software Applications	Network Devices	Host Devices	Embedded Devices
Integrity	Spoofing Identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0888, T0847, T0848, T0885, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	[SPOOFING THROUGH NETWORK DEVICES] Spoofing identities to access and control network device. Techniques: T0819, T0866, T0822, T0883, T0886, T0848, T0862, T0860, T0812, T0866, T0886, T0859, T0830, T0885	[SPOOFING THROUGH HOST DEVICES] Spoofing identities to access and control host device. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0885, T0862, T0864, T0860, T0874, T0856, T0812, T0866, T0867, T0886, T0859, T0885, T0884, T0869, T0856, T0831, T0832	[SPOOFING THROUGH EMBEDDED DEVICES] Most embedded device doesn't have I&A protection, few might have simple password protection, the attack can spoof identities to access with weak/default password or brute force attack. The attacker can also perform MiTM attack or Session hijacking to gain access to embedded device. Techniques: T0883, T0847, T0882, T0864, T0860, T0866, T0812, T0859, T0845, T0885, T0869, T0856, T0831
Integrity	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with Information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[NETWORK DEVICES TAMPERING] -Physically, tamper the network device by switching network or signal wires. Hundred kilometers of cables are distributed along the trackside making access very easy. -Or access the network device by using console port, remote access tools, default/weak password. Then tamper the network configuration. (e.g. Firewall configuration, route table, ACL). Final scenario, tampering the information flow from network to change the network behavior/performance. (e.g. DDoS, DNS poisoning, ARP spoofing). -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. Techniques: T0862, T0823, T0834, T0830, T0885, T0878, T0803, T0804, T0805, T0835, T0838, T0857, T0806, T0836, T0839, T0879, T0813, T0826, T0827, T0828, T0837	[HOST DEVICES TAMPERING] -Tamper the host device and targeting on the OS level, by using trojans/viruses/worms, remote access tools. Then attacker can modify software or data in the host. (e.g. change firewall configuration in interlocking, add/change user data). -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with Information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0807, T0871, T0823, T0874, T0853, T0863, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0835, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[EMBEDDED DEVICES TAMPERING] -Tamper the embedded device to change its function against the intended purpose. -Disturbance due to radiation: Attacker causes EMI affecting the network cabling or connected devices of the wireless network interfaces. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with hardware: Attacker injects a fault into a hardware of a TCMS device after gaining physical access to the device. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. Techniques: T0862, T0858, T0807, T0821, T0834, T0889, T0873, T0843, T0845, T0885, T0869, T0800, T0878, T0803, T0804, T0805, T0809, T0835, T0838, T0851, T0857, T0806, T0836, T0839, T0856, T0855, T0879, T0813, T0826, T0828, T0837, T0880, T0831
Integrity	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	[REPUDIATION THROUGH NETWORK DEVICES] -Intercept and redirect communication flows related to evidence of afflicting actions to deny faulty actions. Deleting or changing network device log data. (e.g., delete detected attack events on Firewall or IDS/IPS). -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0820, T0830, T0885, T0878, T0803, T0804, T0805, T0814, T0816, T0835, T0838, T0881, T0857, T0806, T0836, T0839, T0879, T0813, T0826, T0837	[REPUDIATION THROUGH HOST DEVICES] Deleting or changing host log data or altering monitoring services to deny faulty actions. (e.g. attacker gains admin privilege and close/disable audited service). Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0820, T0872, T0849, T0851, T0856, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0835, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	[REPUDIATION THROUGH EMBEDDED DEVICES] -Modifying the embedded device which holds evidences of afflicting actions to deny faulty actions. -Interception of compromised interference signals: Attacker intercepts radiation emitted by wireless devices. -Disturbance due to radiation: Attacker causes EMI affecting the network cabling or connected devices of the wireless network interfaces. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0858, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0800, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0835, T0838, T0851, T0881, T0857, T0806, T0836, T0839, T0856, T0855, T0879, T0813, T0828, T0837, T0831
Confidentiality	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	[DISCLOSING INF FROM NETWORK DEVICES] -Spying on a network device to gain confidential information (e.g. passwords, usernames). Gathering information about the system and the surrounding environment by sniffing the network device. -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. Techniques: T0848, T0862, T0823, T0834, T0839, T0857, T0859, T0840, T0842, T0846, T0888, T0887, T0802, T0830, T0887, T0885, T0882	[DISCLOSING INF FROM HOST DEVICES] -Spy and collect information, some information can be used to analyse application or operation behaviours (e.g. Linux logs). Or steal the confidential data/information directly or target entities. -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0807, T0871, T0823, T0874, T0853, T0863, T0857, T0859, T0846, T0888, T0887, T0802, T0811, T0801, T0861, T0852, T0887, T0885, T0884, T0869, T0831, T0882	[DISCLOSING INF FROM EMBEDDED DEVICES] -Theft of media, embedded device or components (e.g. SD-Cards, storage drives, hardware boards) which can lead to gain information. -Spy and collect information, some information can be used to analyze application or operation behaviors (e.g. PLC logs). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network) -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0862, T0858, T0807, T0821, T0834, T0889, T0839, T0873, T0857, T0859, T0843, T0802, T0868, T0877, T0845, T0885, T0869, T0831
Availability	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[DoS NETWORK DEVICES] -Overload the network device or change parameters to make the network unavailable. (e.g. DDoS attack to overflow a firewall or router). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0823, T0834, T0830, T0885, T0878, T0803, T0804, T0805, T0814, T0816, T0835, T0838, T0881, T0857, T0806, T0836, T0839, T0879, T0813, T0815, T0826, T0827, T0828, T0837	[DoS HOST DEVICES] -Overload the host or make the computer resources exhausted by non-control functionalities. (e.g. trigger Anti-virus software scanning on Windows host which exhausts a lot of CPU and memory resources). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0807, T0871, T0823, T0874, T0853, T0863, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0835, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	[DoS EMBEDDED DEVICES] -Destruction of media or embedded device which leads to physical damage to a system or its components that prevents or obstructs the intended use of it. -Overload the embedded device to make the function unavailable. (e.g. DDoS attack). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0858, T0807, T0821, T0834, T0843, T0845, T0885, T0869, T0800, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0835, T0838, T0851, T0881, T0857, T0806, T0836, T0839, T0856, T0855, T0879, T0813, T0826, T0828, T0837, T0880, T0831
Confidentiality	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0885, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	[EoP NETWORK DEVICES] -Abuse of rights while using the network device to affect the network in harmful way or gaining more privileges than originally allowed by using a host vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0819, T0866, T0822, T0883, T0886, T0848, T0862, T0860, T0823, T0834, T0839, T0857, T0859, T0890, T0812, T0866, T0886, T0859, T0830, T0885	[EoP HOST DEVICES] -Abuse of rights while using the host to affect the system in harmful way or gaining more privileges than originally allowed by using a host vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0885, T0862, T0864, T0860, T0807, T0871, T0823, T0853, T0863, T0857, T0859, T0890, T0874, T0812, T0866, T0867, T0886, T0859, T0885, T0884, T0869, T0855, T0831	o

Table 36: Threat Landscape

Function (Primary Asset)	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] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-01 Virtual Coupling Set Up	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-01 Virtual Coupling Set Up	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	3	1	3
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-03 Supervision Train Separation Distance	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 37: Threat Scenarios (1/7)

PA-03 Supervision Train Separation Distance	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-03 Supervision Train Separation Distance	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-03 Supervision Train Separation Distance	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	4	1	4
PA-03 Supervision Train Separation Distance	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-03 Supervision Train Separation Distance	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	4	2	8
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	2	1	2
PA-04 Termination of Virtual Coupling Session	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-05 Calculating Relative Distance between Trains	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 38: Threat Scenarios (2/7)

PA-05 Calculating Relative Distance between Trains	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-05 Calculating Relative Distance between Trains	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-05 Calculating Relative Distance between Trains	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-05 Calculating Relative Distance between Trains	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	2	1	2
PA-05 Calculating Relative Distance between Trains	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-06: Maintaining Headway Between Trains	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-06: Maintaining Headway Between Trains	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-06: Maintaining Headway Between Trains	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-06: Maintaining Headway Between Trains	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	4	1	4
PA-06: Maintaining Headway Between Trains	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-06: Maintaining Headway Between Trains	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	4	2	8
PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 39: Threat Scenarios (3/7)

PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	1	1	1
PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-07 Determining Common Reference for VC Movements Monitoring	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	1	2	2
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-09 Auxiliary Vehicle Functions	VCTS-OB	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 40: Threat Scenarios (4/7)

PA-09 Auxiliary Vehicle Functions	VCTS-OB	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-09 Auxiliary Vehicle Functions	VCTS-OB	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-09 Auxiliary Vehicle Functions	VCTS-OB	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	3	1	3
PA-09 Auxiliary Vehicle Functions	VCTS-OB	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	2	1	2
PA-09 Auxiliary Vehicle Functions	VCTS-OB	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	3	2	6
PA-01 Virtual Coupling Set Up	VCTS-TS	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-01 Virtual Coupling Set Up	VCTS-TS	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-01 Virtual Coupling Set Up	VCTS-TS	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-01 Virtual Coupling Set Up	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 41: Threat Scenarios (5/7)

PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	3	1	3
PA-02 Transition from ATP/Driver supervision to VCTS supervision	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-03 Supervision Train Separation Distance	VCTS-TS	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-03 Supervision Train Separation Distance	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-03 Supervision Train Separation Distance	VCTS-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-03 Supervision Train Separation Distance	VCTS-TS	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	4	1	4
PA-03 Supervision Train Separation Distance	VCTS-TS	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-03 Supervision Train Separation Distance	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	4	2	8
PA-05 Calculating Relative Distance between Trains	VCTS-TS	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8

Table 42: Threat Scenarios (6/7)

PA-05 Calculating Relative Distance between Trains	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-05 Calculating Relative Distance between Trains	VCTS-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-05 Calculating Relative Distance between Trains	VCTS-TS	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-05 Calculating Relative Distance between Trains	VCTS-TS	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	2	1	2
PA-05 Calculating Relative Distance between Trains	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Spoofing identity	[SPOOFING THROUGH SOFTWARE APPLICATIONS] Spoofing identities to access signalling software application. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0874, T0856, T0866, T0867, T0886, T0859, T0845, T0885, T0884, T0869, T0856, T0831, T0832	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Tampering with data	[SOFTWARE APPLICATIONS TAMPERING] -Tamper the signalling software application or support application to work against the intended purpose of the system. -Tamper the configuration during installing or operation. -Data from untrustworthy sources: Software updates for TCMS devices are taken from unreliable repositories which can contain manipulated software. -Tampering with software: Attacker manipulates software of TCMS devices. -Tampering with information: Attacker intercepts, manipulates, and sends out data frames after obtaining access to the TCMS network. -Use of counterfeit or copied software: Counterfeit software is downloaded to TCMS network- or end-devices. -Corruption of data: Attacker gains access to TCMS devices via the network and corrupts/modifies data. -Malicious software: Malicious software is downloaded to TCMS devices. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0843, T0845, T0885, T0884, T0869, T0878, T0803, T0804, T0805, T0809, T0838, T0851, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Repudiation	[REPUDIATION THROUGH SOFTWARE APPLICATIONS] -Deleting or changing software application log data or altering monitoring services to deny faulty actions. -Denial of actions: Data on device has been changed, but it can't be determined by whom. Techniques: T0862, T0821, T0820, T0872, T0849, T0851, T0856, T0843, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0826, T0837, T0831	Integrity	4	2	8
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Information disclosure	[DISCLOSING INF FROM SOFTWARE APPLICATIONS] -Spy and collect information, some information can be used to analyse application or operation behaviours, some information stored in application is confidential, and have direct impact to business. (e.g. Personal information, like name, phone number etc...). -Remote spying: Attacker sniffs data traffic after obtaining remote access to the network (for example by intrusion through the MAR). -Eavesdropping and reconnaissance: Attacker sniffs data traffic after obtaining local access to the network (for example by gaining physical access to the network). -Theft of media, equipment, or documents: Attacker steals one or more TCMS devices after gaining physical access to them. -Disclosure: Attacker reads out confidential content for example diagnostic information after obtaining access to the network. -Fraudulent copying of software: Attacker steals software or credentials after obtaining access to the TCMS. Techniques: T0848, T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0843, T0802, T0811, T0868, T0877, T0801, T0861, T0845, T0852, T0885, T0884, T0869, T0831, T0882	Confidentiality	2	1	2
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Denial of Service	[DoS SOFTWARE APPLICATIONS] -Changes to data that lead to inability to read or process the stored information. Overload the software or change parameters to make the application unavailable. (e.g. fuzzing attacks, buffer overflow attacks, network DoS attack to a specific interface, or lock user's account). Denial of service: Attacker jams the TCMS network or floods devices with requests. Techniques: T0862, T0871, T0823, T0874, T0821, T0853, T0863, T0843, T0845, T0885, T0869, T0878, T0803, T0804, T0805, T0809, T0814, T0816, T0838, T0851, T0881, T0857, T0806, T0836, T0856, T0855, T0879, T0813, T0815, T0826, T0827, T0828, T0837, T0880, T0829, T0831, T0832	Availability	4	1	4
PA-08 Establishing/Monitoring Communication Across a Platoon	VCTS-TS	Elevation of Privilege	[EoP SOFTWARE APPLICATIONS] -Abuse of rights while using the software to affect the system in harmful way or gaining more privileges than originally allowed by using a software vulnerability. -Unauthorised physical access: Attacker gains access to the TCMS (e.g., through stolen maintenance devices or by hacking the MAR from his smart phone or via the internet). -Unauthorised use of equipment: Attacker gains access to the remote maintenance ports or WLAN and compromises the TCMS. -Malicious software: Malicious software is downloaded to TCMS devices. -Abuse of rights: If passwords cannot be changed (are hard-coded) then an attacker may use credentials obtained long ago to still get access to the TCMS. -Forging of rights: Attacker gains access or higher privileges on TCMS devices or subnetworks due to missing or poor password management. Techniques: T0817, T0819, T0866, T0822, T0883, T0886, T0847, T0848, T0865, T0862, T0864, T0860, T0871, T0823, T0821, T0853, T0863, T0889, T0873, T0857, T0859, T0890, T0874, T0866, T0867, T0843, T0886, T0859, T0845, T0885, T0884, T0869, T0855, T0831	Confidentiality	2	2	4

Table 43: Threat Scenarios (7/7)

REFERENCES

[1] S. Chadwick, U. Golebniak, C. LOEFFLER, T. Roman, M. Kemkemer and U. Schöni, “Traffic CS System Concept, v1.5,” Europe’s Rail Joint Undertaking, Brussels, 2025.

[2] M. Prins and B. Simoni, “Train CS Architecture Baseline 1 v1.1,” Europe’s Rail Joint Undertaking, Brussels, 2024.

[3] J. Felez and M. A. Vaquero-Serrano, “Virtual Coupling in Railways: A Comprehensive Review,” 2023.

[4] X2Rail-3, “Deliverable D6.1 Virtual Train Coupling System Concept and Application Conditions,” Shift2Rail, 2020.

[5] ERTMS International, “ERTMS/ETCS,” 2024.

[6] SCOTT, “Full Project Proposal,” VIRTUAL VEHICLE, 2017.

[7] Cordis, “CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes. Phase 1,” [Online]. Available: https://cordis.europa.eu/project/id/730539.

[8] Cordis, “Secure COnnected Trustable Things,” [Online]. Available: https://cordis.europa.eu/project/id/737422.

[9] Cordis, “CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS. PhAse 2.,” [Online]. Available: https://cordis.europa.eu/project/id/826098.

[10] Cordis, “Advanced Signalling, Automation and Communication System (IP2 and IP5) –,” [Online]. Available: https://cordis.europa.eu/project/id/826141.

[11] Cordis, “MOving block and VIrtual coupling New Generations of RAIL signalling,” [Online]. Available: https://cordis.europa.eu/project/id/826347.

[12] Cordis, “Intelligent Secure Trustable Things,” [Online]. Available: https://cordis.europa.eu/project/id/876038.

[13] Cordis, “CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS PhAse 3,” [Online]. Available: https://cordis.europa.eu/project/id/101014811.

[14] S. regulation, “Reglamento de Circulación Ferroviaria,” [Online]. Available: http://www.boe.es/boe/dias/2015/07/18/pdfs/BOE-A-2015-8042.pdf,.

[15] T. B. J.M. Borky, Effective Model-Based Systems Engineering..

[16] P.Roques, Systems Architecture Modeling with the Arcadia Method. A Practical Guide to Capella..

[17] S. Danilo Iovinoa,, N. Ricevutoa, S. Canesia, F. Parrilla Ayusob and G. Lanillos Carrasco, “Virtually Coupled Train Sets: Requirements Specification for ETCS,” 2023.

[18] InSecTT, “Full Project Proposal,” Shift2Rail, 2020.

[19] MOVINGRAIL, “Deliverable D3.1. Virtual Coupling Communication Solutions Analysis,” Shift2Rail, 2018.

[20] MOVINGRAIL, “Deliverable D3.3 Proposals for Virtual Coupling Communication Structures,” Shift2Rail, 2018.

[21] CONNECTA, “D2.3 – Validation Plan and Report for the T2G System,” Shift2Rail, 2018.

[22] CONNECTA 2, “D8.4 – Final report on the contribution of CONNECTA-2 to Shift2Rail,” Shift2Rail, 2021.

[23] Technical Committee : ISO/IEC JTC 1/SC 7, *ISO/IEC/IEEE 29148:2018,* 2018.

[24] X2RAIL3, “Deliverable D6.1 Virtual Train Coupling System Concept and Application,” Shift2Rail, 2020.

[25] X2RAIL3, “Deliverable D7.4 Impact Analysis,” Shift2Rail, 2021.

[26] E. Quaglietta and R. Goverde, “Exploring Virtual Coupling: operational principles and analysis,” in *10th ASPECT Conference of the Institution of Railway Signalling Engineers*, 2019.

[27] European Union Agency for Railways, “System Requirements Specification, SUBSET-026, Issue:4.0.0,” 2023.

[28] MOVINGRAIL, “Deliverable D1.1 Report on Moving Block Operational and Engineering Rules,” Shift2Rail, 2020.

[29] European Union Agency for Railways, “System Requirements Specification, SUBSET-026, Issue:3.6.0,” 2016.

[30] OCORA, “Introduction to OCORA, OCORA-BWS03-010, Version: 6.20,” OCORA Cooperation, 2023.

[31] OCORA, “CCS On-Board (CCS-OB) Architecture, OCORA-TWS01-035, Version: 4.00,” OCORA Cooperation, 2023.

[32] EUG & EULYNX partners, “Commitment to RCA (reference CCS architecture) for future ERTMS rollout., Document id: RCA.Doc.41,” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2019.

[33] EUG & EULYNX partners, “Release notes - RCA Baseline 1 Release 0, Document id: RCA.Doc.5,” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2020.

[34] EUG & EULYNX partners, “RCA System Architecture - Preliminary issue, Document id: RCA.Doc.35, Version: 0.3 (0.A),” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2021.

[35] EUG & EULYNX partners, “RCA Terms and Abstract Concepts, Document ID: RCA.Doc.14, Version: 1.1,” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2022.

[36] European Union Agency for Railways, “System Requirements Specification, SUBSET-036, Issue: 3.1.0,” 2015.

[37] T. Schygulla, J. Reißaus, P. Gamm, P. Hoffmeister and A. Totzauer-Stange, “Balise technology in practice at DB Netz AG,” *SIGNAL+DRAHT,* 12 2020.

[38] DB Netze, “European Train Control System (ETCS) Informationen zu ETCS und der Migration zur europäischen Zugbeeinflussungstechnik bei der DB Netz AG,” DB Netz AG, Frankfurt am Main, 2018.

[39] International union of railways (UIC), “GSM-R - Global System for Mobile communications - Railways,” [Online]. Available: https://uic.org/rail-system/telecoms-signalling/article/gsm-r. [Accessed 30 November 2023].

[40] M. Pannu, R. Bird, B. Gill and K. Patel, “Investigating vulnerabilities in GSM security,” in *International Conference and Workshop on Computing and Communication (IEMCON)*, 2015.

[41] International union of railways (UIC), “FRMCS - Future Railway Mobile Communication System,” [Online]. Available: https://uic.org/rail-system/telecoms-signalling/frmcs. [Accessed 30 November 2023].

[42] EU Member States, “EU coordinated risk assessment of the cybersecurity of 5G networks,” NIS Cooperation Group, 2019.

[43] M. Barros Lourenço, L. Marinos and L. Patseas, “ENISA Threat Landscape for 5G Networks,” ENISA - European Union Agency for Cybersecurity, Heraklion, 2020.

[44] G. Milenkovic and M. Dekker, “5G Supplement - To the Guideline on Security Measures,” ENISA - European Union Agency for Cybersecurity, Heraklion, 2021.

[45] European Conference of Postal and Telecommunications Administrations - CEPT, “CEPT Report 76,” CEPT, Copenhagen, 2020.

[46] ETSI, “Rail Communications (RT),” 2023. [Online]. Available: https://www.etsi.org/technologies/rail-communications. [Accessed 30 November 2023].

[47] X2RAIL3, “Deliverable D7.5 Business Model,” Shift2Rail, 2021.

[48] STARS, “Deliverable D5.1 State of the art of EGNSS projects for the rail,” European Global Navigation Satellite Systems Agency (GSA), 2017.

[49] X2RAIL2, “Deliverable D3.1 System Requirement Specification of the Fail-Safe Train,” Shift2Rail, 2018.

[50] ASTRAIL, “Deliverable D1.6 Proposed GNSS Minimum Performance Requirements,” Shift2Rail, 2019.

[51] J. Marais, J. Beugin and M. Berbineau, “A survey of GNSS-based Research and Developments for the European railway Signaling,” *IEEE Transactions on Intelligent Transportation Systems,* pp. vol. 18 (10): pp 2602-2618, 2017.

[52] R2DATO, “Deliverable D21.1 Operational requirements and system capabilities of an ASTP system (Use Cases),” 2025.

[53] PERFORMINGRAIL, “Deliverable D1.1 Baseline System Specification and Definition for Moving Block Systems,” Shift2Rail, 2021.

[54] Localisation Working Group (LWG), “LOC-OB System Definition & Operational Context, Version: 1,2,” 2023.

[55] X2RAIL3, “Deliverable D7.1 Feasibility Study,” Shift2Rail, 2021.

[56] European Union Agency for Railways, “Glossary of Terms and Abbreviations, SUBSET-023, Issue:4.0.0,” 2023.

[57] X2RAIL2, “Deliverable D4.1 Train Integrity Concept and Functional Requirements Specifications,” Shift2Rail, 2020.

[58] X2RAIL2, “Deliverable D4.2 Functional architecture & Interfaces specifications & Candidate technologies selection,” Shift2Rail, 2020.

[59] R2DATO, “D19.1 – Train Integrity and Train Length Architecture & Functional Requirements,” 2023.

[60] E. H. O. P. H. R. R. F. a. A. W. K. Kuchar, “Hunting Network Anomalies in a Railway Axle Counter System,” *Sensors,* pp. vol. 23, no. 6, p. 3122, 2023.

[61] X2RAIL3, “Deliverable D7.2 System Functional Architecture Specification,” Shift2Rail, 2021.

[62] X2RAIL4, “Deliverable D7.2 OTI Technology Migration,” Shift2Rail, 2023.

[63] J. Pachl, Railway Signalling Principles: Edition 2.0, 2021.

[64] ERA, “Technical Specifications for Interoperability (TSIs) | European Union Agency for Railways,” 1 October 2018. [Online]. Available: https://www.era.europa.eu/domains/technical-specifications-interoperability_en. [Accessed 27 March 2025].

[65] *Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (recast) (Text with EEA relevance),* vol. 138, 2016.

[66] R2DATO, *D21.1 Operational needs and system capabilities of an ASTP system (Use Cases),* 2023.

[67] R2DATO, *D21.2 System requirements of ASTP system,* 2023.

[68] R2DATO, *D22.1 ASTP Report on Common Overall Design and Architecture,* 2024.

[69] R2DATO, *D27.2 Specification of Digital Register Implementation(s) required in R2DATO,* 2023.

[70] R2DATO, *D27.1 Set of requirements on the Digital Register in R2DATO,* 2023.

[71] R2DATO, *D48.4 Technology development of Short Range Communications (SRC) and Relative Localisation (RL),* 2024.

[72] “Springer Handbook of Global Navigation Satellite Systems,” Cham, 2017.

[73] “Position, navigation, and timing technologies in the 21st century: integrated satellite navigation, sensor systems, and civil applications,” Hoboken, 2021.

[74] A. Neri, “Train Control and Rail Traffic Management Systems,” in *Position, Navigation, and Timing Technologies in the 21st Century*, John Wiley & Sons, Ltd, 2020, p. 1811–1838.

[75] P. D. Groves, Principles of GNSS, inertial, and multisensor integrated navigation systems, 2nd ed., Boston: Artech House, 2013.

[76] L. Lo Presti and S. Sabina, GNSS for rail transportation: challenges and opportunities, Cham: Springer, 2018.

[77] “Operating Rules and Interoperability in Trans-National High-Speed Rail,” Cham, 2022.

[78] D. Chen, Intelligent Processing Algorithms and Applications for GPS Positioning Data of Qinghai-Tibet Railway, Berlin, Heidelberg: Springer Berlin / Heidelberg, 2019.

[79] F. Gustafsson, Statistical Sensor Fusion, Lund, Sweden: Studentlitteratur, 2010.

[80] S. Särkkä, Bayesian filtering and smoothing, Cambridge, UK: Cambridge University Press, 2013.

[81] M. Guerrieri, Fundamentals of Railway Design, Cham: Springer Nature Switzerland, 2023.

[82] J. Otegui, A. Bahillo, I. Lopetegi and L. E. Díez, “A Survey of Train Positioning Solutions,” *IEEE Sensors Journal,* vol. 17, p. 6788–6797, October 2017.

[83] M. Hecht, “Railway Systems–Railway Engineering,” in *Springer Handbook of Mechanical Engineering*, K. Grote and H. Hefazi, Eds., Cham, Springer International Publishing, 2021, p. 1057–1083.

[84] O. Plan, *GIS-gestützte Verfolgung von Lokomotiven im Werkbahnverkehr,* Munich, Germany, 2004.

[85] O. Heirich, *Localization of Trains and Mapping of Railway Tracks,* 2020.

[86] O. Heirich, “Bayesian Train Localization with Particle Filter, Loosely Coupled GNSS, IMU, and a Track Map,” *Journal of Sensors,* vol. 2016, p. Article ID 2672640, 2016.

[87] H. Winter, *Ortung von Schienenfahrzeugen und Kartierung von Bahntrassen unter Ausnutzung geometrischer Trassierungselemente,* Darmstadt, 2022.

[88] D. Stein, *Mobile laser scanning based determination of railway network topology and branching direction on turnouts,* Karlsruhe, 2018.

[89] F. Böhringer, Gleisselektive Ortung von Schienenfahrzeugen mit bordautonomer Sensorik, Erscheinungsort nicht ermittelbar: KIT Scientific Publishing, 2008.

[90] S. Hensel, Wirbelstromsensorbasierte Lokalisierung von Schienenfahrzeugen in topologischen Karten, Print on demand ed., vol. 18, Karlsruhe: KIT Scientific Publishing, 2011.

[91] C. Hasberg, Simultane Lokalisierung und Kartierung spurgeführter Systeme, Print on demand ed., vol. 19, Karlsruhe: KIT Scientific Publishing, 2012.

[92] M. Spindler, *Ferromagnetische Inhomogenitäten zur berührungslosen Bestimmung der Geschwindigkeit und gleisselektiven Position von Schienenfahrzeugen,* Karlsruhe, 2021.

[93] R. D. Burns, S. Elliott-Bryan and D. B. Turner, "Rail vehicle positioning system". Patent 5129605A, 14 July 1992.

[94] S. S. Saab, "A map matching approach for train positioning. I. Development and analysis," *IEEE Transactions on Vehicular Technology,* vol. 49, p. 467–475, March 2000.

[95] S. S. Saab, G. E. Nasr and E. A. Badr, "Compensation of axle-generator errors due to wheel slip and slide," *IEEE Transactions on Vehicular Technology,* vol. 51, p. 577–587, May 2002.

[96] S. Hensel, C. Hasberg and C. Stiller, "Probabilistic Rail Vehicle Localization With Eddy Current Sensors in Topological Maps," *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, p. 1525–1536, December 2011.

[97] C. Hasberg, S. Hensel and C. Stiller, "Simultaneous Localization and Mapping for Path-Constrained Motion," *IEEE Transactions on Intelligent Transportation Systems,* vol. 13, p. 541–552, June 2012.

[98] M. Lauer and D. Stein, "A Train Localization Algorithm for Train Protection Systems of the Future," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, p. 970–979, April 2015.

[99] D. Lu and E. Schnieder, "Performance Evaluation of GNSS for Train Localization," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, p. 1054–1059, April 2015.

[100] J. Beugin, C. Legrand, J. Marais, M. Berbineau and E.-M. El-Koursi, "Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control," *IEEE Access,* vol. 6, p. 9898–9916, 2018.

[101] W. Jiang, S. Chen, B. Cai, J. Wang, W. ShangGuan and C. Rizos, "A Multi-Sensor Positioning Method-Based Train Localization System for Low Density Line," *IEEE Transactions on Vehicular Technology,* vol. 67, p. 10425–10437, November 2018.

[102] W. Jiang, Y. Yu, K. Zong, B. Cai, C. Rizos, J. Wang, D. Liu and W. Shangguan, "A Seamless Train Positioning System Using a Lidar-Aided Hybrid Integration Methodology," *IEEE Transactions on Vehicular Technology,* vol. 70, p. 6371–6384, July 2021.

[103] J. Liu, B.-G. Cai, J. Wang and D.-B. Lu, "GNSS Jamming Detection and Exclusion for Trustworthy Virtual Balise Capture in Satellite-Based Train Control," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, p. 23640–23656, December 2022.

[104] D. Liu, W. Jiang, B. Cai, O. Heirich, J. Wang and W. Shangguan, "Robust train localisation method based on advanced map matching measurement-augmented tightly-coupled GNSS/INS with error-state UKF," *The Journal of Navigation,* vol. 76, p. 316–339, March 2023.

[105] M. Roth, J. Heusel, K. Kiyanfar, A. Wenz, S. Ohrendorf-Weiss, P. Mendes, N. Dütsch and A. Martin, "On-board Vehicle Localisation with GNSS and Map Data in the EGNSS MATE Project," *SIGNAL + DRAHT,* vol. 2024, p. 44–50, 2024.

[106] K. Lüddecke and C. Rahmig, “Evaluating multiple GNSS data in a multi-hypothesis based map-matching algorithm for train positioning,” in *2011 IEEE Intelligent Vehicles Symposium (IV)*, 2011.

[107] K. M. Betts, T. J. Mitchell, D. L. Reed, S. Sloat, D. P. Stranghoener and J. D. Wetherbee, “Development and operational testing of a sub-meter Positive Train Location system,” in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, 2014.

[108] M. Roth, B. Baasch, P. Havrila and J. Groos, “Map-Supported Positioning Enables In-Service Condition Monitoring of Railway Tracks,” in *2018 21st International Conference on Information Fusion (FUSION)*, 2018.

[109] H. Winter, V. Willert and J. Adamy, “Increasing Accuracy in Train Localization Exploiting Track-Geometry Constraints,” in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018.

[110] M. Roth and H. Winter, “An Open Data Set for Rail Vehicle Positioning Experiments,” in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 2020.

[111] B. Kröper, M. Lauer and M. Spindler, “Using the Ferromagnetic Fingerprint of Rails for Velocity Estimation and absolute Localization of Railway Vehicles,” in *2020 European Navigation Conference (ENC)*, 2020.

[112] O. Heirich, B. Siebler, A. Lehner, T. Strang and S. Sand, “Magnetic Train Localization: High-Speed and Tunnel, Experiment and Evaluation,” 2022.

[113] L. W. Group, *Train Positioning Techniques’ Comparison,* 2024.

[114] M. Roth, Advanced Kalman Filtering Approaches to Bayesian State Estimation., vol. 1832, Linköping: Linköping University Electronic Press, 2017.

[115] M. Roth, G. Hendeby and F. Gustafsson, “Nonlinear Kalman Filters Explained: A Tutorial on Moment Computations and Sigma Point Methods,” *Journal of Advances in Information Fusion,* vol. 11, p. 47–70, 2016.

[116] J. B. Rawlings, D. Q. Mayne and M. Diehl, Model Predictive Control: Theory, Computation, and Design, 2nd edition ed., Santa Barbara: Nob Hill Publishing, LLC, 2024.

[117] International Electrotechnical Commission, “IEC Technical Specification 61375-2-4,” 9 February 2017. [Online]. Available: https://webstore.iec.ch/en/publication/31865. [Accessed 14 April 2025].

[118] R. C. (. Éric Fontanel (Hg.), Rolling Stock in the Railway System Vol. 1, vol. 1, Global Rail Group, 2020.

[119] R. u. S. M. Radhakrishnan, “Optimization algorithm for minimizing railway energy consumption in hybrid powertrain architectures: A direct method approach using a novel two-dimensional efficiency map approximation,” *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit.*

[120] A. Rupp, M. Steinberger and M. Horn, “Sliding-Mode-Based Platooning: Theory and Applications,” in *Studies in Systems, Decision and Control*, Springer International Publishing, 2020, p. 393–431.

[121] K. Mullankuzhy, *Sliding Mode Controller Design for Gap Control in Virtual Coupling of Rail Vehicles,* Stuttgart, 2023.

[122] R. u. M. K. Parise, “Virtually Coupled Trains Dynamics and Energy Efficiency: A Simulation-Based Analysis,” in *Civil-Comp Press. The Sixth International Conference on Railway Technology: Research, Development and Maintenance*, Prague, 2024.

[123] S. F. &. S. F. Capgemini, “QUANTIFICATION OF THE AERODYNAMIC GAIN ON,” *International Journal of Computational Methods and Experimental Measurements,* 2022.

[124] R. u. D. H. u. W. J. u. L. A. Parise, “Reasoning Functional Requirements for Virtually Coupled Train Sets: Communication.,” *IEEE Communications Magazine,* 2019.

[125] 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].

[126] R. Kour, A. Patwardhan, A. Thaduri and R. Karim, “A review on cybersecurity in railways,” *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit,* vol. 237, no. 1, pp. 3-20, 2023.

[127] European Union Agency for Cybersecurity, ENISA threat landscape 2024: July 2023 to June 2024, Publications Office of the European Union, 2024.

[128] X2RAIL-5, “Deliverable D11.1 Cybersecurity assessment of other TD’s,” Shift2Rail, 2023.

[129] “ISA/IEC 62443 Series of Standards,” [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 27 August 2024].

[130] “CLC/TS 50701:2023 Railway applications - Cybersecurity,” CENELEC, [Online]. Available: https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/. [Accessed 27 September 2024].

[131] “The STRIDE Threat Model,” Microsoft Corporation, [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20). [Accessed 3 July 2024].

[132] “Common Vulnerability Scoring System SIG,” Forum of Incident Response and Security Teams, [Online]. Available: https://www.first.org/cvss/. [Accessed 9 December 2024].

[133] ERTMS Users Group, “SECURITY,” [Online]. Available: https://ertms.be/activities/ertms-security-core-group. [Accessed 3 July 2024].

[134] X2RAIL-5, “Deliverable D14.3 Support of the Europe’s Rail SP with Cyber Security Topics – Part 1 Risk Assessment,” Shift2Rail, 2024.

[135] X2RAIL3, “Deliverable D8.1 Guidelines for Railway Cybersecurity Design, Implementation on the Railway Sign. System,” Shift2Rail, 2020.

[136] EUG & EULYNX partners, “RCA Architecture Poster - Preliminary issue - With OCORA contribution, Document id: RCA.Doc.40, Version: 1.0 (0.A),” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2022.

[137] EUG & EULYNX partners, “APS Detailed concepts overview, Document ID: RCA.Doc.52, Version: 1.0,” RCA (an initiative of the ERTMS Users Group and EULYNX Consortium), 2022.

[138] X2RAIL3, “Deliverable D7.4 - Impact Analysis,” 2018.

[139] STARS, *D5.1 State of the art of EGNSS projects for the rail application,* 2017.

[140] R2DATO WP27, *D27.1 – Set of requirements on the Digital Register in R2DATO,* 2023.