OCORA

Open CCS On-board Reference Architecture

System Architecture

Document ID: OCORA-TWS01-030

Version: 2.01

Release: R1

Date: 03.12.2021

Management Summary

This document is the 5th edition of the OCORA System Architecture. It represents a significant step forward towards an open, modular, exchangeable, migratable, evolvable, and portable CCS On-Board System. Whilst considering economical aspects, modular safety, as well as cyber-security and sector feedback, a reasonable number of plug-and-play like building block candidates have been identified.

The development of the OCORA System Architecture follows an iterative approach, evolving within the progress of the OCORA collaboration. With this release, OCORA made its second step towards using Model Based Systems Engineering (MBSE) based on the Arcadia methodology.

OCORA has started using the Capella MBSE tool for developing the logical architecture, well knowing that the Arcadia methodology proposes to start with the operational- and system-analysis before diving into the development of the logical architecture. It has been a deliberate decision to deviate from the Arcadia proposed approach for the following reasons:

1. The CCS On-Board system is considered a sub-system of the overall CCS system which includes CCS on-board and CCS trackside. OCORA favours the development of the operational- and system-analysis on a system and not on a sub-system level. This is to ensure the proper development of the end-to-end functionality and to minimize integration efforts at a later stage. The close collaboration with RCA (responsible for the overall CCS system architecture) for developing system capabilities has just started but OCORA aims to develop and communicate its ideas for the CCS On-Board in parallel. This can be done best through a high-level logical and physical architecture.
2. The CCS On-Board system is a well-known system that exists today and is already documented to a certain extent on a logical- and physical architectural level. Starting from this status quo architecture and applying the OCORA Guiding Principles [8], the OCORA Stakeholder-Requirements [25], the OCORA Program-Requirements [26], and the OCORA Design-Requirements [27] has dramatically accelerated the development of an initial versions of the OCORA System Architecture. The currently proposed logical and physical architecture will be iteratively adjusted and concluded once functions are being allocated to logical components (typically after completion of the system analysis phase). During the latter process, new logical components may evolve, some may be combined, and others may disappear entirely.
3. OCORA aims to develop its CCS On-Board architecture in close collaboration with other programs and sector initiatives (e.g., RCA, TOBA, EEIG ERTMS UG LWG, CONNECTA, LinX4Rail, X2Rail-4, UNISIG/UNIFE, etc.). Most of these programs have not yet performed and documented the operational- and systems-analysis but have developed a logical and/or physical architecture. To fit in the overall railway / CCS landscape and to facilitate understanding and communication between the different programs, OCORA adopts logical and physical components from other programs wherever reasonable. Adjustments will be performed iteratively at different points in time, concluding in a final logical architecture after completion of the functional allocation process.

Moving forward, OCORA plans to collaborate very closely with RCA and other programs in performing the system analysis and developing the system capabilities including functional chains and scenarios.

The currently proposed logical architecture is also and especially a result of the collaboration work with RCA, EUG-LWG and X2Rail-4. The alignment on the actors has reached quite a good level and alignment work on the logical components has started. The OCORA logical architecture will continue to evolve alongside with the developments in the mentioned programs.

The currently proposed physical architecture is also a result of the collaboration work with UIC TOBA regarding connectivity and S2R CONNECTA regarding on-board communication. The OCORA physical architecture will continue to evolve alongside with the developments in those programs and incorporate changes due to the advancing logical architecture.

The allocation of logical components to hardware is one of the last steps in the Arcadia methodology and will be performed by OCORA once the functional allocation to logical components is concluded. During that process new physical components may evolve, some may be combined, and others may disappear entirely.

Revision history

Version	Change Description	Initial	Date of change
1.04	Official version for OCORA Delta Release	AL	30.06.2021
1.05	Improved quality of graphics	AL	09.07.2021
2.01	Official version for OCORA Release R1	AL	03.12.2021

Table of contents

Table of figures

Table of tables

References

Reader's note: please be aware that the numbers in square brackets, e.g., [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g., SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS02-030 – Technical Slide Deck

[6] OCORA-BWS02-050 – Technical Posters

[7] OCORA-BWS03-010 – Introduction to OCORA

[8] OCORA-BWS03-020 – Guiding Principles

[9] OCORA-BWS04-010 – Problem Statements

[10] OCORA-BWS08-010 – Methodology

[11] OCORA-TWS01-010 – System Requirements

[12] OCORA-TWS01-040 – Capella Modelling

[13] OCORA-TWS01-050 – Capella Model Export

[14] OCORA-TWS01-100 – Localisation On-Board (LOC-OB) – Introduction

[15] OCORA-TWS01-101 – Localisation On-Board (LOC-OB) – Requirements

[16] OCORA-TWS01-112 – Automatic Train Protection On-Board (ATP-OB) – MLM Interface Analysis

[17] OCORA-TWS02-010 – CCS Communication Network – Evaluation

[18] OCORA-TWS02-020 – CCS Communication Network – Proof of Concept (PoC)

[19] OCORA-TWS03-010 – Computing Platform – Whitepaper

[20] OCORA-TWS03-020 – Computing Platform – Requirements

[21] OCORA-TWS04-010 – Functional Vehicle Adapter – Introduction

[22] OCORA-TWS04-011 – Functional Vehicle Adapter – Requirements

[23] OCORA-TWS04-012 – Functional Vehicle Adapter – Standard Communication Interface Specification

[24] OCORA-TWS04-013 – Functional Vehicle Adapter – Design Guideline

[25] OCORA-TWS05-020 – Stakeholder Requirements

[26] OCORA-TWS05-021 – Program Requirements

[27] OCORA-TWS05-022 – Design Requirements

[28] OCORA-TWS06-010 – (Cyber-) Security – Project Security Management Plan

[29] OCORA-TWS06-020 – (Cyber-) Security – Guideline

[30] RCA.Doc.35 – RCA System Architecture, BL0, R2, Version 0.2 (0.A), Sprint 22, 2021-05-29

[31] RCA.Doc.40 – RCA Poster, BL0, R2, Version 0.2 (0.B), Sprint 22, 2021-05-27

[32] X2Rail-4 – Deliverable D3.2 – GoA3/4 Specification, Version 0.1.1, 2021-06-17

[33] EN 50126-1:2017-10 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[34] EN 50126-2:2017-10 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[35] EN 50128:2011-06 – Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems

[36] EN 50129:2018-11 – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[37] EN 50155: 2017 – Railway applications – Rolling stock – Electronic equipment

[38] EN 50159:2010-09 – Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[39] TSI CCS: 02016R0919 - EN - 16.06.2019 - 001.001 - 1: COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union, amended by Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 L 139I

[40] ISO/IEC 7498-1:1994, Information technology – Open Systems Interconnection — Basic Reference Model: The Basic Model - Part 1.

[41] ERA_ERTMS_015560 – ETCS Driver Machine Interface

[42] EUG 97E2675B – ERTMS User Group Document 97E2675B

[43] EN 15380-4 – Railway applications - Classification system for railway vehicles - Function groups

[44] UIC, Future Railway Communications System, User Requirements Specification, FU-7100

1 Introduction

1.1 Purpose of the document

The purpose of this document is to document and communicate the current state of the OCORA reference architecture. The document is focusing on technical issues and possible solutions for the CCS On-Board system. It aims at providing the best possible technical solution, without considering imbalances of costs and benefits between On-Board and trackside that may arise due to the proposed solutions.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for On-Board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete On-Board CCS system, or also for On-Board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing On-Board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant CCS On-Board solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of the OCORA Release R1, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [7], and the Problem Statements [9]. The reader should also be aware of the Glossary [2] and the Question and Answers [3]. Information about the Capella modelling are available in document [12].

Further details on technical aspects of the OCORA proposed solution are provided in the following documents:

- The CCS Communication Network – Evaluation [17]
- CCS Communication Network – Proof of Concept (PoC) [18]
- Computing Platform – Whitepaper [19]
- Computing Platform – Requirements [20]
- Functional Vehicle Adapter – Introduction [21]
- Functional Vehicle Adapter – Requirements [22]
- Functional Vehicle Adapter – Standard Communication Interface Specification [23]
- Functional Vehicle Adapter – Design Guidelines [24]
- (Cyber-) Security – Guidelines [29]

1.4 Useful information for the readers

All Capella graphics depicted in this document are available in Capella native format in [13]. Selected graphics depicted in this document are available, in a larger scale, in the documents [5] and [6], and in Appendix D.

1.5 Notations

OCORA is using the Arcadia methodology and the Capella application for MBSE. Therefore, the graphics depicted in this document follow the notations used by Capella.

Interfaces labelled in green (CCS-OB external) or red (CCS-OB internal) are planned to be defined by OCORA, together with other organisations that have interest in the respective interface definition (e.g., RCA, X2R4, EUG-LWG, etc.).

Interfaces labelled in blue are defined by RCA in cooperation with OCORA, where applicable. Interfaces labelled in black are outside the OCORA scope.

For the identification of interfaces, the following notation is used:

Notation	Description
CI-xxx	Communication Interface
HMI-xxx	Human Machine Interface
HWI-xxx	Hardware Interface
PI-xxx	Perception Interface
SAI	Standard Authentication/Authorisation Interface
SCI-xxx	Standard Communication Interfaces
SDI	Standard Diagnostic Interface
SMI	Standard Maintenance Interface
SS-nnn	ERTMS Subset
(SS-nnn)	Subset used as input for IF specification

Table 1 Notation for interface identification

2 System under consideration

2.1 Scope

OCORA has developed a logical architecture (Figure 1) and a physical architecture (Figure 2) to identify the OCORA collaboration scope for the architectural work. Both views identify the CCS-OB (green box) with the respective context (actors and external systems). A brief description of the actors and external systems can be found in chapter 2.2, a description of the logical components in chapter 2.3 and the physical components in chapter 2.4.

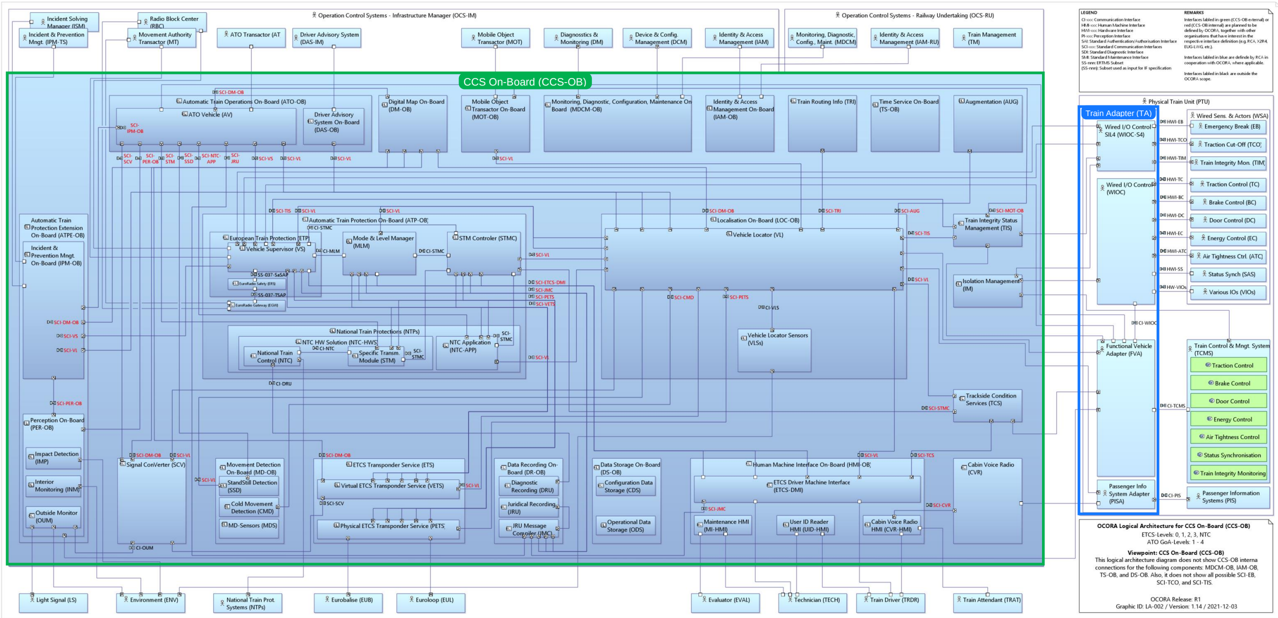

Figure 1 Scope – logical view

(refer to Appendix D4 for large scale representation)

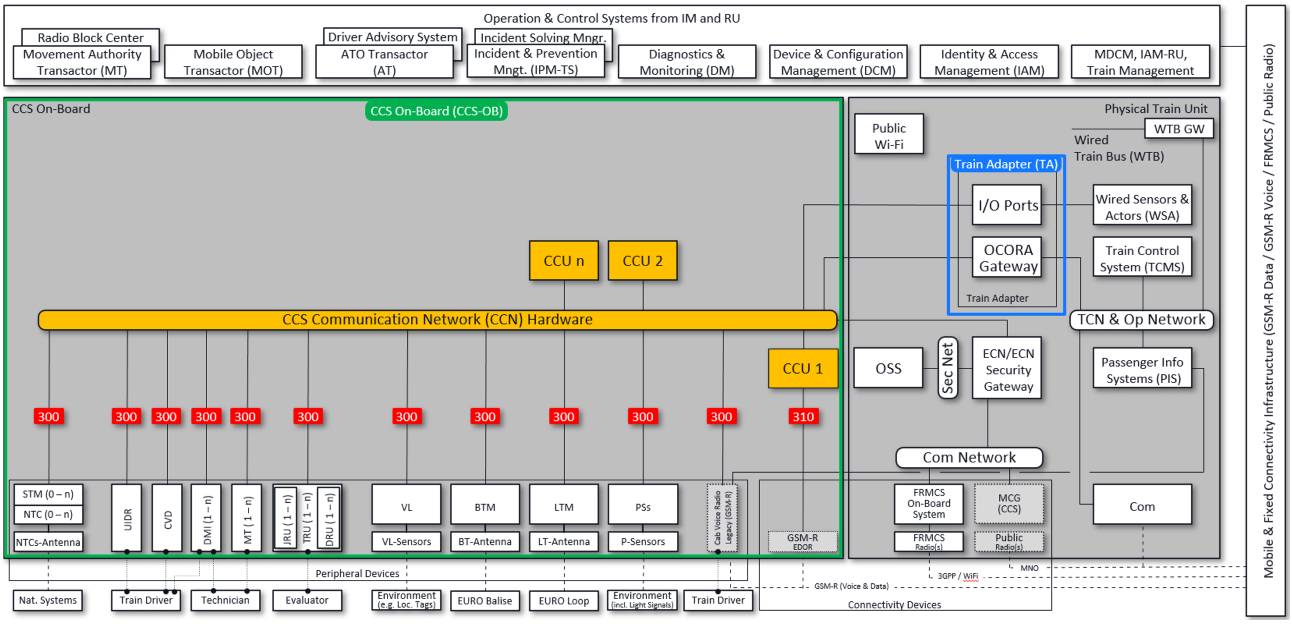

Figure 2 Scope – physical view

(refer to Appendix D2 for large scale representation)

Remark: solid lines indicate wired connections, dotted lines represent user interactions, and dashed lines “over the air” communication

The system under consideration of the OCORA collaboration is CCS-OB (green box) as identified in Figure 1 from a logical perspective and in Figure 2 from a physical point of view. This scope applies to the system decomposition and to all RAMSS aspects and is used for CENELEC phase 1 – 5 and 8 – 12 (refer to OCORA CENELEC interpretation in document [10]).

In addition, OCORA aims at providing requirements, a standardized interface specification, and design guidelines for implementing a Train Adapter (TA). The TA (blue box) is outlined in Figure 1 from a logical perspective and in Figure 2 from a physical point of view. Currently, OCORA works on the specifications of the Functional Vehicle Adapter (FVA), which is a central part of the TA. The respective documentation can be found in:

- Functional Vehicle Adapter – Introduction [21]
- Functional Vehicle Adapter – Requirements [22]
- Functional Vehicle Adapter – Standard Communication Interface Specification [23]
- Functional Vehicle Adapter – Design Guidelines [24]

This System Architecture document is focussing on the CCS On-Board (CCS-OB) scope only. The Train Adapter (TA) scope is treated in this document as an actor and therefore only discussed in chapter 2.2.4 as part of the Physical Train Unit (PTU) actor.

OCORA aims at providing the architecture for a CCS On-Board (CCS-OB) solution that is compliant with trains equipped with a Next/New Generation – Train Control Network (NG-TCN) while also supporting legacy trains. It further aims at standardizing the CCS-OB in such a way that the same CCS-OB architecture can be used for legacy and NG-TCN based trains. OCORA is using the legacy trains scenario for defining the system under consideration for CCS-OB (scope, context, etc.). Refer to Appendix A for the different scenarios considered at this point in time.

From an OCORA system architecture and design perspective, the focus is on the orange marked parts of the CCS-OB (see Figure 2) and the CCS-OB internal interfaces (red marked in Figure 1 and Figure 2).

To develop the first proposal for the logical and physical architecture, OCORA has identified components for the CCS-OB (blocks inside the green box) using the OCORA Guiding Principles [8], the OCORA Stakeholder-Requirements [25], the OCORA Program-Requirements [26], and the OCORA Design-Requirements [27].

Components are defined as a piece of hardware and/or software, providing one or more functionalities.

Every component can consist of sub-components. All currently proposed logical and physical components are described in more detail in chapter 4 and 5.

As explained in document [7], OCORA aims to introduce “plug & play”-like exchangeability for the CCS On-Board building blocks (refer to chapter 3 for a definition of building blocks). Since efforts to do so are quite extensive, and since OCORA wants to leave as much room as possible to the industry to provide their (already existing) solutions, OCORA uses building blocks to group components. Building blocks can contain 1 - n component(s). It is the OCORA vision to provide “plug & play”-like exchangeability for all building blocks (refer to chapter 3) and not for all components as identified in Figure 1 and in Figure 2.

The components within the CCS-OB as identified in Figure 1 and Figure 2 support ETCS L0 – L3, level NTC, ATO GoA1 – GoA4 over ETCS (refer to requirement OCORA-58 in [25]), GSM-R and/or FRMCS connectivity, and the potential to implement NNTRs (Notified National Technical Rules). ETCS is the primary ATP, hence always present (refer to requirement OCORA-56 in [25])

The configuration for a specific implementation is open and may include only a subset of the components represented in Figure 1 and Figure 2. But not only the number of deployed components can differ between implementations. The functionality of some of the physical components (Figure 2) may vary also. For example: on one vehicle the CCU 1 could contain the ETCS functionality and CCU 2 the ATO functionality, while another supplier may decide to use CCU 1 for combined ETCS and ATO functionality and use CCU 2 as a fail-over unit to increase availability of the CCS-OB system. Yet another specific implementation may combine all safe functions on CCU 1 and all non-safe functions on CCU 2. To achieve this, the independence of software from hardware is paramount and therefore an important topic to OCORA. Refer to chapter 9, document [19], and [20] for details on the computing platform, that supports the separation of hardware from software.

The components identified in Figure 1 and Figure 2 represent just a high-level view, abstracting many details. For example: The CCN, shown as a single block, is in fact a complex component with many sub-components and configuration options, depending on the needs of the RU/supplier (refer to Appendix B).

Last but not least, the representation in Figure 1 and Figure 2 show, as already mentioned, one possible deployment scenario (scenario 1 as per Appendix A); especially regarding the OCORA Gateway (OCORA-GW) and how the connectivity devices (GSM-R Radio, Public Radio, FRMCS Radio) and the train networks (TCN, Operator Network) are connected.

All identified components, and external systems are described further in subsequent chapters of this document. Chapter 2.3 provides a list and a short description of all logical components, including references to more detailed information and chapter 2.4 provides the same for physical components.

To define the architecture of the CCS-OB to the necessary detail, all envisioned interfaces are identified from a physical point of view and on a logical level. Equally, for the external interfaces (refer to chapter 6) and the internal interfaces (refer to chapter 7). Specifications for the identified interfaces will be provided in a later version of the OCORA documentation.

2.2 Actors

All currently identified actors and their interfaces with the CCS-OB are identified in Figure 3 from a logical and in Figure 4 from a physical perspective. All actors are briefly described in the subsequent chapters.

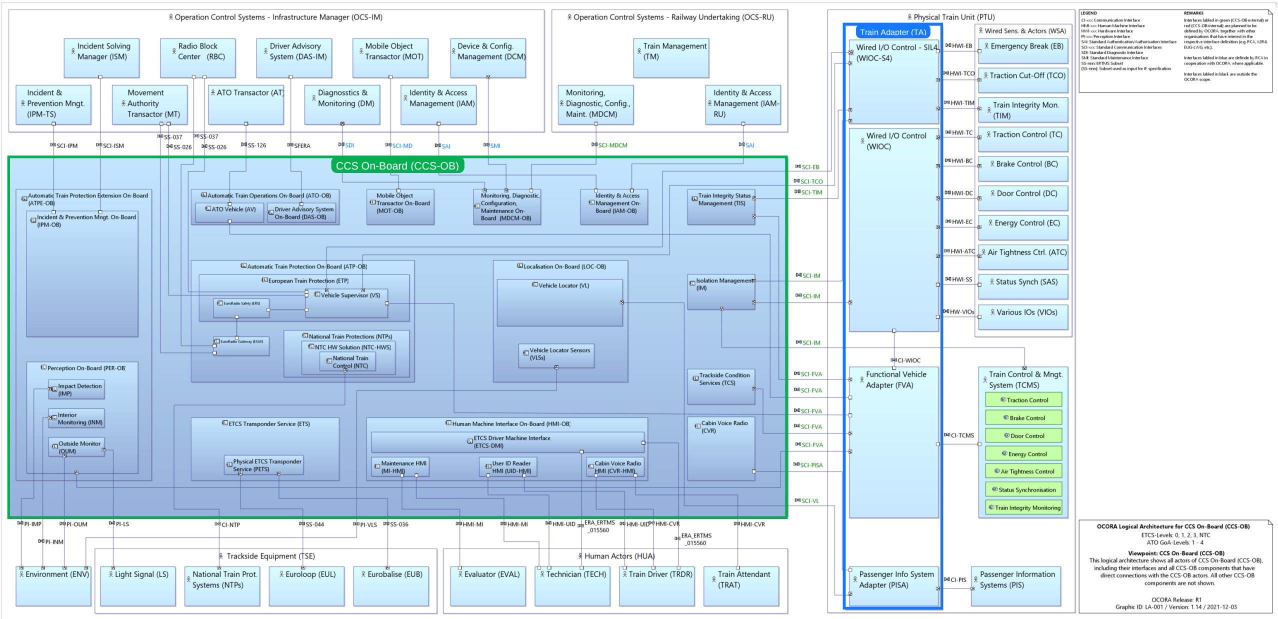

Figure 3 CCS-OB actors – logical perspective

(refer to Appendix D3 for large scale representation)

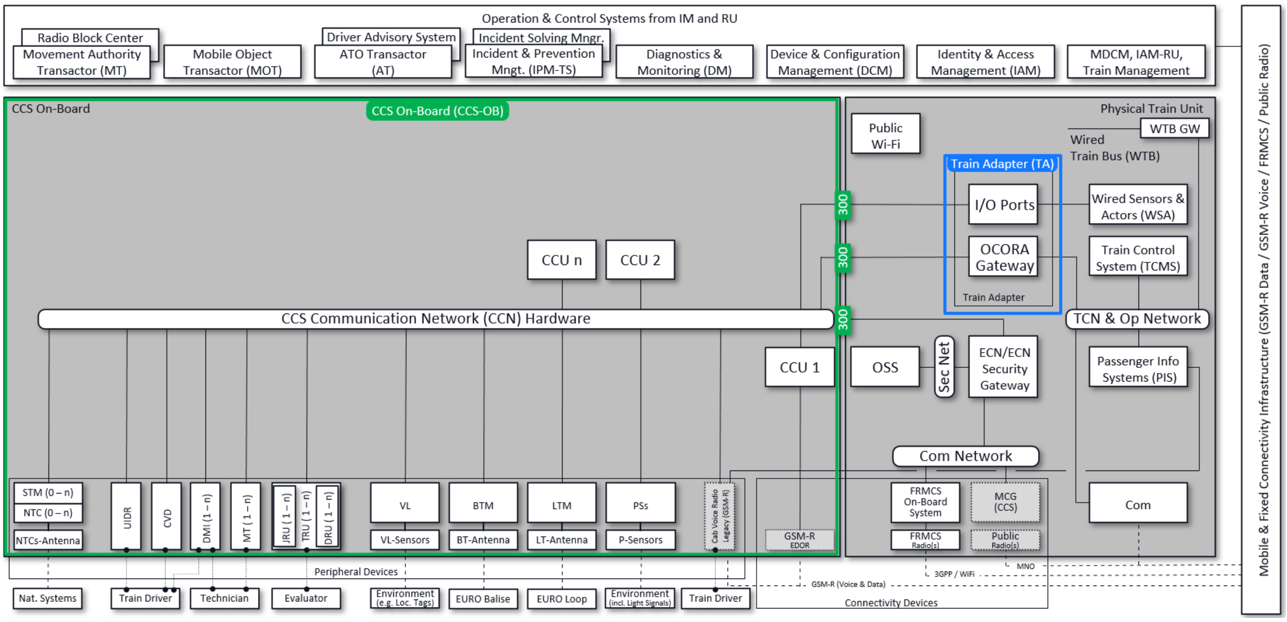

Figure 4 CCS-OB actors – physical perspective

(refer to Appendix D1 for large scale representation)

2.2.1 Human Actors (HUA)

The Human Actors (HUA) are the users of the CCS On-Board (CCS-OB) system. The actors currently identified, including their roles, are listed in Table 2.

Actor	Abbreviation	Role
Train Attendant	TRAT	A Train Attendant is personnel of the Railway Undertaking that is escorting the Passenger Train. The Train Attendant is responsible for Passenger service and Train service. (see also RCA definition as per document [30])
Train Driver	TRDR	A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible, and safe manner. Source: Directive 2007/59/EC of the European Parliament and of the Council. (see also RCA definition as per document [30])
Technician	TECH	The person performing preventive and corrective maintenance tasks.
Evaluator	EVAL	The person evaluating data stored in the TRU and the DRU.

Table 2 Actors - Human Actors (HUA)

2.2.2 Environment (ENV)

The actor Environment (ENV) represents the environment around the CCS-OB. Sensors and video cameras interface with the environment.

Actor	Abbreviation	High-Level Description	Link to Interface Description
Environment	ENV	Environment provides information about conditions, influencing the railway operation. It can be trackside or vehicle based. (see also RCA definition as per document [30])	PI-OUM PI-INM PI-IMP PI-VLS

Table 3 Actors - Environment (ENV)

2.2.3 Trackside Equipment (TSE)

Trackside Equipment (TSE) are the systems installed at trackside, interacting with the CCS-OB system, using the interface(s) referenced in Table 4.

Actor	Abbreviation	High-Level Description	Link to Interface Description
Euroloop	EUL	A transponder loop mounted along the track, which can communicate with a train passing along, compliant to the ERTMS/ETCS specifications.	SS-044
Eurobalise	EUB	A transponder, mounted on the track, which can communicate with a train passing over it, compliant to the ERTMS/ETCS specifications.	SS-036
National Train Protection Systems	NTPs	Any kind of national Automatic Train Protection (ATP) system.	CI-NTP
Light Signal	LS	The railway light signals.	PI-LS

Table 4 Actors - Trackside Equipment (TSE)

2.2.4 Physical Train Unit (PTU)

The Physical Train Unit (PTU) includes all systems of the train that interact directly or through the Train Adapter (TA) with the CCS On-Board. For this actor, we distinguish between the logical and physical aspects.

2.2.4.1 Logical aspects of the Physical Train Unit (PTU)

The logical Train Adapter (TA) is a part of the Physical Train Unit (PTU) and connects the CCS On-Board with the TCMS, PIS, and WSA, using the interface(s) referenced in Table 5.

Actor	Abbreviation	High-Level Description	Link to Interface Description
Train Control Management System	TCMS	The Train Control Management System typically includes the following functionalities, relevant for CCS-OB: ▪ Traction Control ▪ Brake Control ▪ Door Control ▪ Energy Control ▪ Air Tightness Control ▪ Status Synchronisation ▪ Train Integrity Monitoring The TCMS connects to the CCS-OB through the FVA, using the PTU internal CI-TCMS interface. In addition, there is direct interface (SCI-IM) between the TCMS and the Isolation Management component (IM) of the CCS-OB.	SCI-IM CI-TCMS
Passenger Information Systems	PIS	The Passenger Information System (PIS) typically includes the following functionalities, relevant for CCS-OB: ▪ Passenger announcement from the operation control center of the IM or the RU (OCS-IM, OCS-RU), the Train Driver (TRDR), or the Train Attendant (TRAT) ▪ Communication between Train Driver (TRDR) and Train Attendant (TRAT) ▪ Providing position and speed information to passengers The Passenger Information System connects through the PISA, using the PTU internal CI-PIS interface. Remark: The PIS does not include the network provided for passenger internet services.	CI-PIS
Wired Sensors & Actors	WSA	Wired Sensors and Actors (WSA) are directly used and activated on legacy trains with no TCMS or with a TCMS with limited functionality. The Wired Sensors and Actors (WSA) connect to the CCS-OB through the WIOC and WIOC-S4. **SIL4 components:** ▪ Emergency Break (EB) using interface HWI-EB ▪ Traction Cut-Off (TCO) using interface HWI-TCO ▪ Train Integrity Monitoring (TIM) using interface HWI-TIM **SIL<4 components:** ▪ Traction Control (TC) using interface HWI-TC ▪ Brake Control (BC) using interface HWI-BC ▪ Door Control (DC) using interface HWI-DC ▪ Energy Control (EC) using interface HWI-EC ▪ Air Tightness Control (ATC) using interface HWI-ATC ▪ Status Synch (SAS) using interface HWI-SS ▪ Various I/Os (VIOs) using interface HWI-VIOs	HWI-EB HWI-TCO HWI-TIM HWI-TC HWI-BC HWI-DC HWI-EC HWI-ATC HWI-SS HWI-VIOs

Actor	Abbreviation	High-Level Description	Link to Interface Description
Train Adapter	TA	The Train Adapter (TA) includes all components enabling access between the CCS-OB and the systems of the Physical Train Unit (PTU) that are relevant for CCS-OB.	HWI-EB HWI-TCO HWI-TIM HWI-TC HWI-BC HWI-DC HWI-EC HWI-ATC HWI-SS HWI-VIOs SCI-EB SCI-TCO SCI-TIM SCI-IM SCI-FVA SCI-PISA SCI-VL
.. Wired I/O Control SIL4	WIOC-S4	The Wired I/O Control SIL4 (WIOC-S4) provides connectivity between SIL4 Wired Sensors and Actors and the CCS-OB. Triggering the emergency brake, cutting the traction, or reporting the integrity of the train are typical functions integrated through the WIOC-S4, as long as no SIL4 TCMS is available. The isolation signal (SCI-IM) is used to bypass the failsafe states of the Wired I/O in case the ETCS On-Board gets isolated.	SCI-EB SCI-TCO SCI-TIM SCI-IM HWI-EB HWI-TCO HWI-TIM
.. Wired I/O Control	WIOC	The Wired I/O Control (WIOC) provides connectivity between Wired Sensors and Actors with SIL<4 and the CCS-OB through the FVA.	SCI-IM CI-WIOC HWI-TC HWI-BC HWI-DC HWI-EC HWI-ATC HWI-SS HWI-VIOs
.. Functional Vehicle Adapter	FVA	The Functional Vehicle Adapter (FVA) is a piece of software deployed on the OCORA computing platform, on a separate computing unit, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardised interface (SCI-FVA) for the OCORA Software to access vehicle functions and vehicle information. Furthermore, it uses a specific interface (SCI-VL) to provide localisation information to the TCMS. Although the TSI-CCS SUBSET-034, SUBSET-119, and SUBSET-139 are defining the interface to the TCMS system, vehicles from different suppliers and especially from different generations have still different interfaces implemented. This adapter allows to map, on a functional level, the commands sent, and the information received from a specific TCMS into the OCORA standard. This includes that the FVA can likewise be used to integrate vehicles through wired connections. **Remark:** Sometimes the FVA is also called Train Interface Unit (TIU). However, the TIU is not clearly defined. Sometimes it refers to the functional level of the interface with the vehicle, while in another context a piece of hardware is meant. To avoid confusion, OCORA does not use the term TIU.	SCI-FVA SCI-VL CI-TCMS CI-WIOC Document: [21], [22], [23], [24]
.. Passenger Info System Adapter	PISA	The Passenger Information System Adapter (PISA) is a non-safe piece of software deployed on the OCORA computing platform, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardised interface (SCI-PISA) towards the Cabin Voice Radio (CVR), allowing the PISA to receive CCS information of interest to the PIS.	SCI-PISA SCI-VL CI-PIS

Table 5 Actors - Physical Train Unit (PTU)

2.2.4.2 Physical aspects of the Physical Train Unit (PTU)

The physical Train Adapter (TA) is a part of the Physical Train Unit (PTU) and connects the CCS On-Board with the physical train. It consists of I/O Ports and in case of an integration into a legacy vehicle, the OCORA Gateway.

I/O Ports

The I/O Ports provide access between the CCN and certain actuators and sensors. The status of the sensors is processed by this component and made available on the CCN and commands from the various CCS On-Board components, sent through the CCN, are applied to the respective port.

This component will provide I/O Ports up to SIL4 required by ETCS and possibly other applications like, NTC-APP, ATPE-OB, etc to trigger the Emergency Brake, Traction Cut-Off and to retrieve the status of the Train Integrity Monitoring.

The I/O Ports are installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the I/O Ports component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

OCORA Gateway (OCORA-GW)

The OCORA Gateway (OCORA-GW) is a piece of hardware providing communication capabilities between the CCN and the legacy Train Control Network (if it exists) or the TCMS (if it exists) or the legacy actuators and sensors residing outside the CCS domain but important to CCS. Depending on the vehicle, the OCORA Gateway covers multiple OSI layers (refer to OCORA OSI definitions in document [10]). This can include even layer 7 in some cases. The OCORA-GW provides a means of integrating the CCS system with various vehicle technologies, especially when deploying an OCORA based CCS system on existing fleets. For situations, where the CCS and the TCN/Op networks are using the same technology and the TCMS implements the standard vehicle adapter interface (SCI-FVA), the OCORA-GW is not needed, and an ECN/ECN Security Gateway ensures security and performance.

The OCORA-GW is installed on every OCORA based CCS On-Board system whilst and where no standardized and common TCMS-CCS network is available. In case there is no TCMS, the CCS can integrate directly with vehicle I/O Ports via the FVA located on the OCORA-GW or on a CCU. Refer to Appendix D1 on page 110 to locate the OCORA-GW component in the OCORA architecture.

Furthermore, the Operator network, depending on security requirements, may also be connected to the Gateway, ensuring communication between the CCS Systems and the Passenger Information Systems.

OCORA aims at defining a standardized CCS System with standardized interfaces. To integrate with the different current and future Train Control and Passenger Information systems without modifying the standardized CCS System, corresponding adapters might be needed to convert standardized OCORA communication protocols and messages to the specific protocols and messages of the respective Train Control and Passenger Information Systems. The Gateway may provide the environment to run the necessary adapters. Once there is a standardized TCMS interface defined, the need for adapters vanishes and the Gateway may not be required anymore. For the interface with the vehicle TCMS, this is specified in document [21], [22], [23] and [24].

While OCORA foresees in its architecture the Gateway for integrating with the specific Train Control and Passenger Information Systems, the implementation of the Gateway remains a vehicle specific integration task. Depending on the specific situation, the OCORA Gateway may be simple or quite complex. In any case, the OCORA Gateway, drawn as a single box in Appendix D1 on page 110, is composed of multiple subcomponents. Some of these sub-components will be part of most OCORA Gateway deployments while others are only needed for some integrations. The purpose, the requirements, and the decomposition of the OCORA Gateway will be discussed in more detail in the upcoming OCORA releases.

ECN/ENC Security Gateway

The ECN/ECN Security Gateway is a network component providing cyber secure interconnection between the different On-Board network zones (e.g., CCS/TCMS, Operator, Connectivity).

The ECN/ECN Security Gateway is installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the ECN/ECN Security Gateway component in the OCORA architecture.

The ECN/ECN Security Gateway monitors and filters all traffic between the connected networks based on the configured security policies (e.g., IP source address, IP destination address, Source port, etc.).

2.2.5 Operations Control Systems – Infrastructure Manager (OCS-IM)

The Operations Control Systems – Infrastructure Manager (OCS-IM) includes all systems of the Infrastructure Manager that interact directly with the CCS On-Board, using the interface(s) referenced in Table 6.

Actor	Abbreviation	High-Level Description	Link to Interface Description
Incident & Prevention Management	IPM-TS	X2Rail-4 definition as per document [32]: The Incident and Prevention Management - Incident Solving Manager (IPM-ISM) component predicts the geographical, temporal and resource-related impact of Events on scheduled railway operation. Solving processes are aligned and prioritised. Specified routines are created to resolve Non-Regular Situations with a minimal impact on railway operation. Planned routines are executed and assisting entities coordinated. An Incident is monitored and managed during his whole lifecycle from the first recognition to the dissolution.	SCI-IPM
Incident Solving Manager	ISM		SCI-ISM
Radio Block Centre	RBC	Definition as per www.wikipedia.org: The Radio Block Centre (RBC) is a specialised computing device with Safety integrity level 4 (SIL) for generating Movement Authorities (MA) and transmitting it to trains. It gets information from Signalling control and from the trains in its section. It hosts the specific geographic data of the railway section and receives cryptographic keys from trains passing in. According to conditions the RBC will attend the trains with MA until leaving the section. RBC have defined interfaces to trains but have no regulated interfaces to Signalling Control and only follow national regulation. The RBC is not part of the RCA architecture, but for migration purposes relevant to OCORA.	SS-026
Movement Authority Transactor	MT	RCA definition as per document [30]: The APS-MT communicates with the registered ETCS capable vehicles. Among others, it translates the movement permissions to ETCS Movement Authorities and send them to the vehicle. Only radio based ETCS is supported. In the other direction it will receive the train position reports from the vehicle and forward them to OA.	SS-026
ATO Transactor	AT	RCA definition as per document [30]: ATO-AT implements the communication with all registered ATO vehicles and provides the standardized interface.	SS-126
Driver Advisory System	DAS-IM	The Driver Advisory System (DAS-IM) application is a non-safe application. It generates, together with the Driver Advisory On-Board (DAS-OB) application, detailed driver advice for adhering to the planned timings while driving energy efficient. The DAS-IM is responsible for conflict detection and calculation of new target train timings, that are forwarded to the Driver Advisory On-Board (DAS-OB) application. The DAS-IM is responsible to calculating an energy efficient speed profile to achieve the pre-planned and dynamically updated train timings. The DAS-IM communicates with the DAS-OB, using the SFERA specification.	SFERA
Mobile Object Transactor	MOT	RCA definition as per document [30]: The APS-MOT manages the different kinds of mobile devices, that are locatable and optionally can be warned. It provides information to the mobile devices, which they need to localize themselves. The MOT processes the received localization information such that it can be forwarded to the OA. It also forwards warning information to the mobile devices.	SCI-MD
Diagnostics & Monitoring	DM	RCA definition as per document [30]: Diagnostics & Monitoring (DM) collects monitoring and diagnostics information from all systems like central systems, trackside assets or the vehicles. The information is on one side used to derive the capacity limitation and an estimated duration of the capacity limitation that is used in TMS to reschedule Capacity Plan. On the other side the information is forwarded to a monitoring system of the Infrastructure Manager, which triggers the corrective maintenance actions. It must be noted that there is the need for a DM system operated by the Infrastructure Manager of the network and a DM operated by the RU of the vehicle, hence the two interfaced identified. More detailed information will be provided in subsequent versions of this document.	SDI

Actor	Abbreviation	High-Level Description	Link to Interface Description
Device & Config Management	DCM	RCA definition as per document [30]: The Device & Configuration Management (DCM) is used to register, setup, and manipulate devices. This includes updating the configuration data and the software version. Safety criticality: DCM is safety critical in so far, that part of the configuration is safety critical. Not the whole DCM needs to be on highest safety levels. It must be noted that there is the need for a DCM system operated by the Infrastructure Manager of the networks and a DCM operated by the RU of the vehicle, hence the two interfaced identified. More detailed information will be provided in subsequent versions of this document.	SMI
Identity & Access Management	IAM	RCA definition as per document [30]: The Identity & Access Management (IAM) authenticates and authorizes users and technical systems and grants or denies access to the system. Therefore, it will need to store the credentials to authenticate the entities. Supports the implementation of an ISO27001 / IEC 62443 compatible architecture. It must be noted that there is the need for an IAM system operated by the Infrastructure Manager of the network and an IAM operated by the RU of the vehicle, hence the two interfaced identified. More detailed information will be provided in subsequent versions of this document.	SAI

Table 6 Actors - Operations Control Systems – Infrastructure Manager

2.2.6 Operations Control Systems – Railway Undertaking (OCS-RU)

The Operations Control Systems – Railway Undertaking (OCS-RU) includes all systems of the Railway Undertaking that interact directly with the CCS On-Board, using the interface(s) referenced in Table 7.

External System	Abbreviation	High-Level Description	Link to Interface Description
Monitoring, Diagnostic, Configuration, Maintenance	MDCM	This trackside logical component provides monitoring, diagnostic, configuration, and maintenance functionality for the CCS-OB.	SCI-MDCM
Identity & Access Management	IAM-RU	The Identity & Access Management (IAM) authenticates and authorizes users and technical systems and grants or denies access to the system. Therefore, it will need to store the credentials to authenticate the entities. Supports the implementation of an ISO27001 / IEC 62443 compatible architecture. It must be noted that there is the need for an IAM system operated by the Infrastructure Manager of the network and an IAM operated by the RU of the vehicle, hence the two interfaced identified. More detailed information will be provided in subsequent versions of this document.	SAI
Train Management (TM)	TM	X2Rail-4 definition as per document [32]: This trackside logical component supervises the train missions, provides the Mission Profile to ATO-AV (remark from OCORA: via AT to AV) and permits remote control actions on TCMS.	

Table 7 Actors - Operations Control Systems – Railway Undertaking

2.3 Logical components

All currently identified logical components of the CCS On-Board are depicted in Figure 5. A high-level description including links to more detailed information for all logical components is provided in the subsequent chapters and a more detailed explanation of the OCORA logical architecture for CCS On-Board is provided in chapter 4.

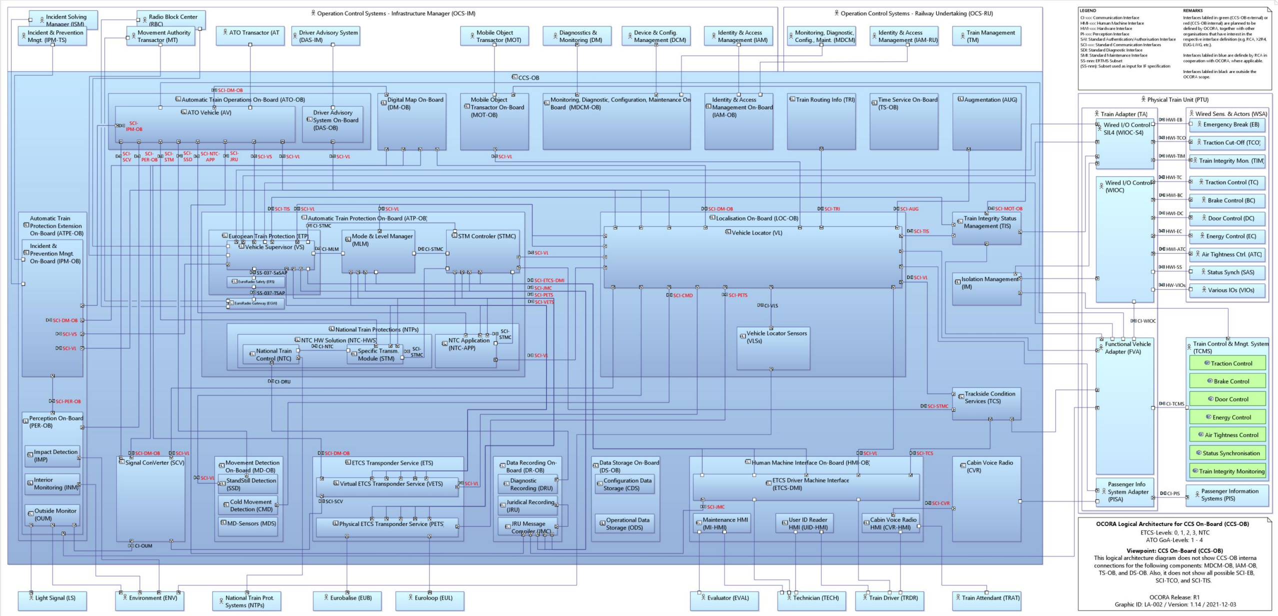

Figure 5 Logical components

(refer to Appendix D4 for large scale representation)

2.3.1 Automatic Train Protection On-Board (ATP-OB)

The logical component ATP-OB includes the functionality needed for the automatic train protection. This includes the functionality of the European Train Protection (ETCS) as well as any functionality needed for National train Protection. Refer to Chapter 4.1 for further Information.

The ATP-OB consists of the subcomponents provided in the table below:

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
European Train Protection	ETP	The logical component ETP contains the VS functionality.	▪ Chapter 4.1.1
.. Vehicle Supervisor	VS	The Vehicle Supervisor (VS) application, deployed on the OCORA computing platform, is a safe ETCS application (mandatory requirements are specified in SUBSET-026) in charge of calculating location specific speed limits (based on various inputs) and activating the braking system in case of speed limit overshoot. Location information is received from the Vehicle Locator (VL). In addition, information is received from the Balise Transmission Module (BTM) and the Loop Transmission Module (LTM) and processed adequately. In ETCS L2 and L3 mode, the VS interacts with the RBC or the APS-MT respectively. It receives the movement authority (MA) and reports the train position (TPR) to the respective system. The VS is agnostic to the communication technology used. Therefore, communication via GSM-R as well as via FRMCS or any future technology is possible. The VS also displays to the driver the necessary information (including cab signalling in ETCS L1, L2 and L3). It supports all ETCS modes and ETCS levels defined in the TSI-CCS.	▪ Chapter 4.1.2

Logical Components			
Component	Abbreviation	High-Level Description	Link to Further Information
.. EuroRadio Safety	ERS	The EuroRadio Safety component represents the safety layer of the EuroRadio Protocol referred as the Safe Functional Module (SFM) in SUBSET-037.	▪ Chapter 4.1.3
EuroRadio Gateway	EGW	The EuroRadio Gateway component implements the layers of SUBSET-037 below the safety layer including coordination between the legacy EDOR and the new On-Board FRMCS as well as the FRMCS client realizing the loose coupling to the services of the On-Board FRMCS.	▪ Chapter 4.1.3
Mode & Level Manager	MLM	The Mode & Level Manager (MLM) is a safe component of the ETCS Core in charge of managing the ETCS modes and levels. It ensures that the proper ETCS mode and level are active and manages the transitions from one mode or level to the other. In the latter context it also handles the handover between different RBCs. Furthermore, it makes sure that the correspondent information (e.g., current mode and level) is transmitted to the TCMS.	▪ Chapter 4.1.4
STM Controller	STMC	The STM Controller (STMC) is a safe component of the ETCS Core in charge of managing the safety authority between ETCS and installed national ATP systems (STM / NTC). It ensures that the proper ATP system is active and manages the switch-over from ETCS to the national ATP system and vice versa. The STMC interacts with the national ATP systems as defined in SUBSET-035 and SUBSET-058. The STMC with the respectively integrated national ATP systems enable an automatic transition from ETCS to the national ATP system and vice versa while the vehicle is driving.	▪ Chapter 4.1.5
National Train Protections	NTPs	The NTPs provides Automatic Train Protection functionality on national level. The NTPs can be either a dedicated NTC HW Solution (NTC-HWS) or it can be deployed as NTC Application (NTC-APP) running on the OCORA computing platform.	▪ Chapter 4.1.6
.. NTC HW Solution	NTC-HWS	The NTC-HWS is a dedicated hardware solution implementing the national Automatic train protection solution with the NTC and STM components.	▪ Chapter 4.1.7
..... National Train Control	NTC	The National Train Control (NTC) implements the national Automatic Train Protection functionality on dedicated hardware. It communicates with other OCORA components, namely the STM and can also use the functionality of other components connected to the CCN (e.g., DRU).	▪ Chapter 4.1.8
..... Specific Transition Module	STM	The Specific Transmission Module (STM) provides the connection between the ETCS system (in case of OCORA the CCN) and the National Train Control System (NTC). The STM and the NTC are often closely integrated, hence the term STM is often used, when referring to the NTC system.	▪ Chapter 4.1.9
.. NTC Application	NTC-APP	The National Train Controls Applications (NTC-APP), deployed on the OCORA computing platform, are safe applications in charge of ensuring Automatic train protection based on national systems. NTC-APPs, implemented on the OCORA computing platform, must communicate, as a minimum, with the Mode and Level Manager (MLM) and can use their specific sensors and actuators. In addition, they can take advantage of the standard OCORA interfaces. E.g., location information can be received from the Vehicle Locator (VL), data can be recorded in the DR-OB, DMI can be used, the TCMS can be accessed through the Functional Vehicle Adapter (FVA) and the NTC-APPs can also access balise telegrams through the ETCS Transponder Service (ETS) in order to get the packet 44 information.	▪ Chapter 4.1.10

Table 8 CCS On-Board logical components – ATB-OB

2.3.2 Automatic Train Protection Extension On-Board (ATPE-OB)

This logical component includes all functionality needed for extending from ATO GoA 1-2 to ATO GoA 3-4.

Refer to Chapter 4.4 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
Incident & Prevention Management On-Board	IPM-OB	X2Rail-4 definition as per document [32]: This logical component is in the train and should substitute Train Driver and Train Attendant responsibilities for reacting in case of an incident (Incident and Prevention Management - Onboard). It manages safe reflexive reactions, computed reactions, and safety procedures in cooperation with IPM-TS and ISM. This logical component is primarily used in case of GoA3/4 but may also assist the train driver in GoA1/2 operations.	▪ Chapter 4.2.1
Perception On-Board	PER-OB	X2Rail-4 definition as per document [32]: The Perception (PER) component is in the train and senses the Physical Railway Environment in place of a driver.	▪ Chapter 4.2.2
.. Impact Detection	IMP	The IMP detects impacts of the train with an object and informs the IPM-OB accordingly (refer also to RCA definition for "SubSys IMP" in document [30]).	▪ Chapter 4.2.3
.. Interior Monitoring	INM	The INM monitors the environment inside the train and informs the IPM-OB about any abnormalities (refer also to RCA definition for "SubSys INT" in document [30]).	▪ Chapter 4.2.4
.. Outside Monitoring	OUM	OUM monitors the environment around the train and informs the IPM-OB about any abnormalities (refer also to RCA definition for "SubSys TFM" in document [30]).	▪ Chapter 4.2.5

Table 9 CCS On-Board logical components – EXATP-OB

2.3.3 Localisation On-Board (LOC-OB)

The logical component LOC-OB contains the VL and VLS functionality.

Refer to Chapter 4.2 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
Vehicle Locator	VL	The Vehicle Locator (VL) is a safe CCS On-Board component that uses sensor data and supporting information to provide train location output information safely and reliably. The Vehicle Locator (VL) is able to provide the absolute and relative position of the front end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles; hence, the VL is more than just an odometry component.	▪ Chapter 4.3.1 ▪ Document [14] ▪ Document [15]
Vehicle Locator Sensors	VLS	This logical component includes the functionality the locator sensors are providing.	▪ Chapter 4.3.2 ▪ Document [14]

Table 10 CCS On-Board logical components – LOC-OB

2.3.4 Automatic Train Operations On-Board (ATO-OB)

This logical component includes all functionality needed for ATO GoA 1-2.

Refer to Chapter 4.4 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
ATO-Vehicle	AV	The ATO Vehicle (AV) application, deployed on the OCORA computing platform, is a non-safe application for Automatic train operations. A safe extension is needed for GoA3 and GoA4 operations. This is provided by the Automatic Train Protection Extension On-Board (ATPE-OB). The AV in GoA2 – GoA4 controls the vehicle's speed, using information received through the interface SS126. It also communicates with the Vehicle Supervisor (VS) over the interface SS130 (between AV and ETCS Core). Remark: AV is called ATO-OB in GoA2 Shift2Rail SUBSET-125.	▪ Chapter 4.4.1
Driver Advisory System On-Board	DAS-OB	The Driver Advisory System On-Board is an optional and non-safe application calculating an energy efficient speed profile to achieve the pre-planned and dynamically updated train timings. It generates detailed driver advice for adhering to the planned timings while driving energy efficient. The trackside Driver Advisory System (DAS-IM) or the Traffic Management System (TMS) is responsible for conflict detection and calculation of new target train timings, that are forwarded to the DAS-OB and evaluated accordingly. The typical integration of DAS-OB application is defined EN 15380-4. The DAS-OB can also operate standalone (e.g., without integration into the vehicle). The DAS-OB is not needed if ATO Vehicle (AV) is installed, since the AV already includes the DAS functionality. The implementation of DAS application on the OCORA computing platform is an open issue to be solved in subsequent versions of this document (unsafe information displayed on the driver DMI).	▪ Chapter 4.4.2

Table 11 CCS On-Board logical components – ATO-OB

2.3.5 Digital Map On-Board (DM-OB)

The logical component DM-OB is a safe service deployed on the OCORA computing platform. The DM-OB provides topology and topography data (a.k.a. map data) that are certified for the usage in safety-relevant On-Board applications / services (e.g., VL, VS, PER-OB) up to SIL4. The service guarantees that the map data fulfils the quality criteria stated by trackside, e.g., accurate, precise, reliable, complete, and up-to-date map data. The DM-OB uses its own On-Board data storage that is updated, if required, using the functionality of the Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB) to propagate trackside map data (e.g., from Topo4) to the On-Board data storage.

Refer to Chapter 4.5 for further Information.

2.3.6 Mobile Object Transactor On-Board (MOT-OB)

The logical component MOT-OB communicates with various CCS On-Board logical components and communicates with the MOT. The need for this component is an open issue to be solved in subsequent versions of this document.

Refer to Chapter 4.6 for further Information.

2.3.7 Monitoring, Diagnostic, Configuration, Maintenance (MDCM-OB)

The logical component MDCM-OB deployed on the OCORA computing platform, collects data relevant for local (through the Maintenance Terminal or DMI) and remote diagnostic and monitoring. For local maintenance, it provides the relevant data upon request to the Maintenance Terminal or DMI in a standardised format. For remote diagnostics and monitoring the data can be sent to multiple recipients (e.g., the RU of the vehicle, the IM the vehicle currently operates in, the vehicle provider, the CCS On-Board provider etc.). The owner of the vehicle can define in the vehicle's configuration (refer to Configuration Data Storage) what data is forwarded to which recipient(s).

The MDCM-OB also allows for local (through the Maintenance Terminal) and remote (through the centralised DCM services) configuration of the vehicle's devices (CCUs, Gateway, Peripherals, etc.). The component can process data received by the IMs (network related operational data) and the RU (vehicle related operational and configuration data). The service also allows the RU to execute commands (e.g., reboot of a specific component) and allows to install updates (e.g., new software).

refer to Chapter 4.7 for further Information.

2.3.8 Identity & Access Management On-Board (IAM-OB)

The Identity & Access Management On-Board (IAM-OB) is a service deployed on the OCORA computing platform. It integrates with the IAM System providing the central management for the identification, authentication and authorisation of devices and applications to resources and functions of the CCS On-Board and trackside systems. For the identification, the IAM System manages a unique ID for each entity (e.g., device, application). The granularity, on what level the system will be split into separate entities is not yet defined. It can reach from one single ID for the overall CCS On-Board system to IDs for any single device connected to the CCN and to application, running on the OCORA Platform. For the authentication of a device or an application, the solution could be based on the Public Key Infrastructure (PKI) or Message Authentication Codes (MAC) using symmetrical encryption mechanisms like 3DES or AES. The access to resources and functions is centrally managed by roles and granted on a Need-to-Know principle to limit unauthorised access to resources and functions within the CCS On-Board system.

Refer to Chapter 4.8 for further Information.

2.3.9 Train Routing Info (TRI)

An interlocked (safe) train path uniquely assigned to a train/vehicle. This information is seen useful to validate the determined position by the Vehicle Locator (VL) against track selectivity.

Refer to Chapter 4.9 for further Information.

2.3.10 Time Service On-Board (TS-OB)

The Time Service On-Board (TS-OB) provides a service that allows all On-Board components to have their time in synch with a master clock and therefore in synch with each other and the trackside systems (e.g., safe data centres). The time base is assumed to be UTC and components in need to display the time can convert it to local time based on the systems time zone settings. The TS-OB functionality is significant to simplify diagnostic and analysis tasks and is important for ATO operations, and other aspects (e.g., used to timestamp the output of the localisation system with the validity time of the information provided).

Refer to Chapter 4.10 for further Information.

2.3.11 Augmentation (AUG)

Augmentation of a positioning system is a method of improving – "augmenting" - the positioning system's performances, such as integrity, accuracy, or availability thanks to the use of external information. (source EUG-S2R JWG).

Refer to Chapter 4.11 for further Information.

2.3.12 Train Integrity Status Management (TIS)

The Train Integrity Status Management is a safe component deployed on the OCORA computing platform or the OCORA gateway. It provides the train integrity status in a standardised fashion to the OCORA software components. To provide the train's integrity status, multiple options are possible:

a) train integrity determination on the train (e.g., through the TCMS),

b) second localisation unit at the end of the train with On-Board determination of the train integrity, and

c) second localisation unit at the end of the train with trackside determination of the train integrity.

The TIS component ensures that all CCS applications that need to know the train's integrity status (including the coupler statuses, if applicable) are receiving the information through a standardised interface, independent of the option used. The train integrity status also includes the total safe train length (including the safe length over coupled compositions).

Refer to Chapter 4.12 for further Information.

2.3.13 Isolation Management (IM)

The logical component IM allows to isolate one or multiple ATP systems and informs the PTU accordingly.

Refer to Chapter 4.13 for further Information.

2.3.14 Trackside Condition Services (TCS)

The Trackside Condition Services (TCS) is a non-safe component of the ETCS Core in charge of managing the trackside condition information received from balises, RIU, or RBC. It calculates the remaining distance to specific trackside points and triggers the appropriate actions according to the location. Location information is received from the Vehicle Locator (VL). Also, the TCS informs the driver about the trackside points: it sends the commands to display the different pictograms on the DMI depending on the trackside point and the relative location to it. Furthermore, it makes sure that the correspondent information is transmitted using the SCI-FVA interface via FVA to the vehicle, and the distance information is updated as needed. The TCS remains active during level transitions, including transition to level NTC.

Refer to Chapter 4.14 for further Information.

2.3.15 Cabin Voice Radio (CVR)

The logical component CVR, deployed on the OCORA computing platform, implements the Cab Voice Radio functionality. The CVR is operated through the CVR-HMI component, which allows the train driver to initiate and receive voice communication between the train and the trackside operations control centres. In some cases, the CVR may also provide the functionalities to communicate with the train staff and to use the Passenger Information System for announcements by using the SCI-PISA interface.

For communication with the trackside operation control centres, the CVR component is using the services provided by the FRMCS On-Board System.

Refer to Chapter 4.15 for further Information.

2.3.16 Human Machine Interface On-Board (HMI-OB)

The logical component HMI-OB includes the functionality needed for any user interaction with the CCS On-Board. This includes the functionality to operate the European Train Protection (ETCS), the Cabin Voice Radio (CVR) as well as any functionality needed for local diagnostics and maintenance of the CCS On-Board. Refer to Chapter 4.16 for further Information.

The HMI-OB consists of the subcomponents provided in the table below:

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
ETCS Driver Machine Interface	ETCS-DMI	The ETCS-DMI component provides the functionality for any user interaction with the ETCS On-Board system.	▪ Chapter 4.16.1
Maintenance HMI	MI-HIM	The MI-HMI component provides the functionality for any user interaction regarding the maintenance of the CCS On-Board.	▪ Chapter 4.16.2
User ID Reader HMI	UID-HMI	The UID-HMI component provides the functionality for any user interaction UID Reader off the CCS On-Board.	▪ Chapter 4.16.3
Cabin Voice Radio HMI	CVR-HMI	The CVR-HMI component provides the functionality for any user interaction with the OCORA based Cab Voice Radio.	▪ Chapter 4.16.4

Table 12 CCS On-Board logical components – HMI-OB

2.3.17 Data Storage On-Board (DS-OB)

The logical component DS-OB provides the functionalities to store and retrieve operational and configuration data used by the CCS On-Board.

Refer to Chapter 4.17 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
Configuration Data Storage	CDS	The Configuration Data Storage (CDS) stores static and semi-static data needed for the CCS On-Board system. The data storage is separated from the operational data and it is separated from the ETCS components (e.g., VS) to make the data easily available to other applications that may need it (e.g., VL). The Configuration Data Storage contains data provided when commissioning a CCS On-Board system for the first time and is changed whenever configurations of the vehicle change (e.g., additional sensors, additional DMI, etc.). The data is entered by service technicians through the local maintenance terminal or via the remote maintenance. In both cases this occurs through the Monitoring, Diagnostic, Configuration, Maintenance (MDCM-OB) component. In subsequent versions of the OCORA specifications, the CDS will be specified in detail.	▪ Chapter 4.17.1
Operational Data Storage	ODS	The Operational Data Storage (ODS) is a data storage for saving quite dynamic data that is entered / provided during an operational day of a vehicle and has no relevance for long-time safeguarding. The operational data storage is separated from the ETCS components (e.g., VS) to make the data easily available to other applications that may need it (e.g., ATO Vehicle). The operational data storage contains data provided by the driver, the TCMS, I/O Ports, and possibly the device and configuration management. Examples of Operational Data is the driver id, the train running number, the status of a cab, etc. In subsequent versions of the OCORA specifications, the ODS will be specified in detail.	▪ Chapter 4.17.2

Table 13 CCS On-Board logical components – DS-OB

2.3.18 Data Recording On-Board (DR-OB)

The logical component DR-OB includes the Juridical Recording Unit (JRU), the Diagnostic Recording Unit (DRU) and the JRU Message Compiler (JMC). Currently, the JRU is mostly located in the CCS domain while the DRU is typically found in the Train Control domain. The JRU records data from the ETCS system while the DRU is recording data from other On-Board systems, for instance the TCMS. In the future, other functions than ETCS will reside in the CCS domain (e.g., ATO). Those functions have also a need to record data. Hence, a DRU is proposed to be added to the CCS domain.

Refer to Chapter 4.18 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
Diagnostic Recording	DRU	The DRU provides data recording mechanisms to applications residing in the CCS On-Board domain. Whether this is a specific hardware, in addition to the hardware available in the TCMS domain, or the DRU hardware can be combined needs to be explored further.	▪ Chapter 4.18.1
Juridical Recording	JRU	The JRU is recording data from the ETCS system.	▪ Chapter 4.18.2
JRU Message Compiler	JMC	The JMC aggregates data from the JRU and compiles them into a human readable format to support efficient data analysis.	▪ Chapter 4.18.3

Table 14 CCS On-Board logical components – DR-OB

2.3.19 ETCS Transponder Service (ETS)

The logical component ETS provides real and/or virtual ETCS transponder messages to the CCS On-Board applications.

Refer to Chapter 4.19 for further Information.

The ETS consists of the subcomponents provided in the table below:

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
Virtual ETCS Transponder Service	VETS	The VETS component generates virtual ETCS telegrams based on the current location using the Digital Map On-Board (DM-OB).	▪ Chapter 4.19.1
Physical ETCS Transponder Service	PETS	The PETS component reads the ETCS telegrams from the trackside installed infrastructure (Eurobalise and Euroloop) and forwards them to the CCS On-Board applications.	▪ Chapter 4.19.2

Table 15 CCS On-Board logical components – ETS

2.3.20 Movement Detection On-Board (MD-OB)

The logical component MD contains the logical components SSD, CMD and MD-Sensors. It provides movement information to various consumers.

Refer to Chapter 4.20 for further Information.

Logical Components			
Component	**Abbreviation**	**High-Level Description**	**Link to Further Information**
	MD-OB		▪ Chapter 4.20
Stand Still Detection	SSD	The logical component SSD is a vehicle-based function that detects if the train is standing still. Depending on the consumer of this information, different levels of stand-still thresholds may apply. Remark from discussions with RCA: The SSD information is needed by the RCA-APS and must be provided by the vehicle. An example is the flank protection. It may be useful that a parked vehicle provides flank protection. The RCS-APS would need to know whether or not a vehicle is parked (SSD signal). There might be other scenarios where SSD information is needed/useful for RCA-APS (some of them already exist today). But for those scenarios it is not sufficient to report v=0, since this information is currently only reported in a resolution of 5 km/h, but RCA-APS would need to have a confirmed v=0 (performance and SIL-level currently unknown).	▪ Chapter 4.20.1
Cold Movement Detection	CMD	The logical component CMD is a vehicle-based function that detects if the train has moved while the CCS-OB system was powered-off. The CMD function is especially needed in the migration phase. In the final phase, where the vehicle is “always on” and “always connected / located”, the function may not be needed anymore. It is under discussion, if CMD should also provide the magnitude of the cold movement (see also CR1345 – Threshold small movements). With the implementation of CR1350 (always connected, always reporting) CMD functionality on the vehicle may not be required anymore.	▪ Chapter 4.20.2
MD-Sensors	MDS	The logical component MDS includes the functionality the movement detection sensors are providing.	▪ Chapter 4.20.3

Table 16 CCS On-Board logical components – MD-OB

2.3.21 Signal Converter (SCV)

The Signal Converter (SCV) is in the train and converts the information coming from optical signals into SUBSET-026 compliant information (refer also to X2Rail-4 definition as per document [32]).

Refer to Chapter 4.21 for further Information.

2.4 Physical components

All currently identified physical components of the CCS On-Board are depicted in Figure 6. A high-level description including links to more detailed information for all logical components is provided in the subsequent chapters and a more detailed explanation of the OCORA logical architecture for CCS On-Board is provided in chapter 5.

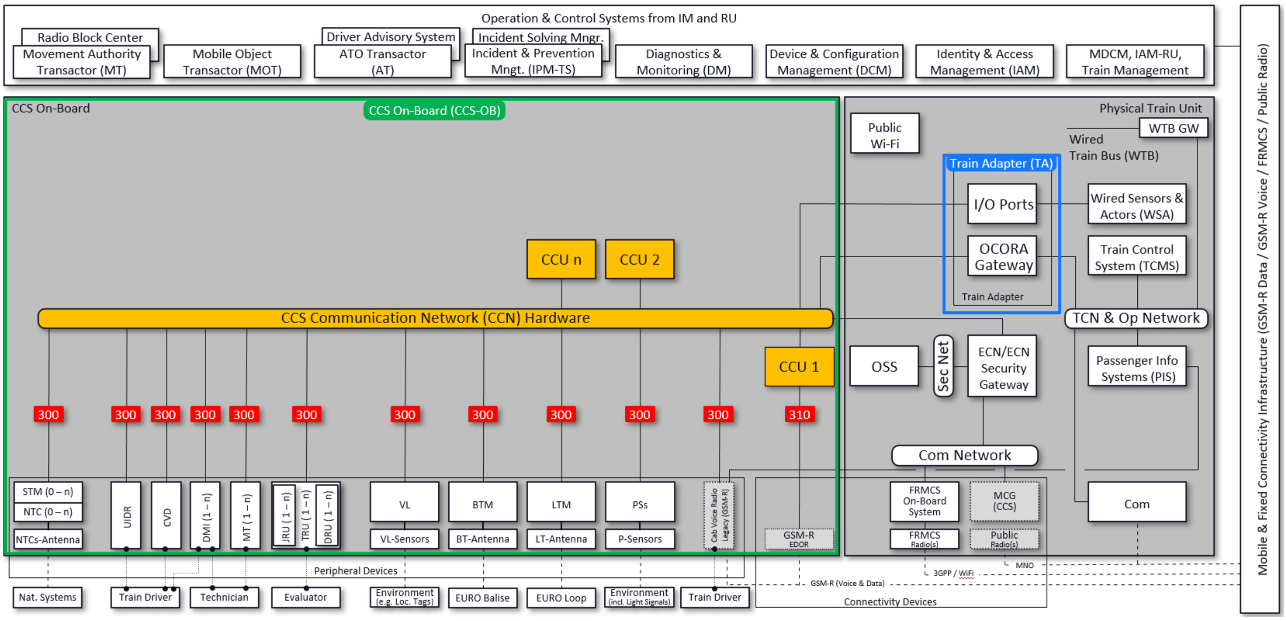

Figure 6 Physical components

(refer to Appendix D2 for large scale representation)

2.4.1 OCORA core hardware

The OCORA core hardware are the components fully filled in orange. The OCORA core hardware, together with the runtime environment (refer to chapter 9), provides the platform to run the OCORA core functionality.

OCORA Core Hardware		
Component	**High-Level Description**	**Link to Further Information**
CCN	**CCS Communication Network** The CCS Communication Network (CCN) allows direct communication between all CCS On-Board components connected to it and eventually with external systems, such as the TCMS. The CCN is the most central part of the OCORA architecture and is the basis for achieving modularity that results in “plug & play”-like exchangeability of all identified building blocks. The CCN is a TSN Ethernet based network with the use of SDTv2/v4 as safety layer. On session layer (OSI layer 5, refer to OCORA OSI definitions in document [10]) different protocols (e.g., TRDP 2.0, OPC UA PubSub over TSN, DDS/RTPS over TSN) are possible. At the final stage, the CCN will be specified on all layers together with Shift2Rail CONNECTA/Safe4RAIL projects in the new IEC 61375 standards series. Refer to document [17] and Appendix B for further details (e.g., the network topology scenarios that OCORA considers for implementing the CCN).	▪ Chapter 5.1.1 ▪ Appendix B ▪ Document [17]

OCORA Core Hardware		
Component	**High-Level Description**	**Link to Further Information**
CCU (1 – n)	**CCS Computing Unit** The CCS Computing Unit (CCU) is the computing hardware for all OCORA core CCS functions. One CCU can contain multiple processor boards (e.g., to provide hardware level voting). The number and the functional behaviour of the CCUs can differ for the various implementations, depending on the RU's need. For migration reasons, multiple CCUs may be needed, or certain functions can be deployed on one node (e.g., safe functions) while others (e.g., non-safe) are deployed on a separate node. In some projects, additional CCUs may be used to increase availability and reliability by defining one or multiple CCU nodes as fail over or standby units. The CCU hardware is made accessible through the runtime environment. The CCU together with the runtime environment are building the computing platform (refer to chapter 9 for details).	▪ Chapter 5.1.2 ▪ Chapter 9 ▪ Document [19]

Table 17 OCORA core hardware

2.4.2 Peripheral devices

The peripheral devices are components outside the "OCORA Core" scope. For these components, OCORA provides interface specifications, high-level functional requirements, and non-functional requirements only. Basically, all requirements and specifications needed to ensure "plug & play"-like exchangeability. Of course, these specifications are only developed for the building blocks not already standardised (well enough) or where no standard is being developed by other organizations. The peripheral devices are also considered for all RAMSS aspects.

The peripheral devices include all sensors and actuators needed for the CCS On-Board system to function and to be able to perform the necessary maintenance tasks.

Peripheral Devices		
Component	**High-Level Description**	**Link to Further Information**
UIDR	**User Identification Reader** The User Identification Reader (UIDR) is used to automate the identification process for drivers and service technicians. RFID card readers may be the most common option used at this point in time. But as technology advances, fingerprint, face ID, etc. might become viable options. The OCORA specifications will be technology agnostic.	▪ Chapter 5.2.1
CVD	**Cabin Voice Devices** The Cabin Voice Devices (CVDs) are the handset, the microphone and the loudspeaker(s) in the cabin, combined with some electronics, allowing to communicate over the CCN with the CVoIP application and ultimately with the FRMCS On-Board System. They are used for the communication between the driver and the operations control personnel or for communication between train staff. Today, these devices are part of a dedicated Cabin Voice Radio and are only loosely integrated into the CCS domain, if at all. But with the upcoming migration from GSM-R to FRMCS options become available to share the new connectivity infrastructure between the CCS data and cabin voice. The OCORA concept foresees to have a cabin voice application running on one of the CCUs and providing voice communication through voice over IP (VoIP).	▪ Chapter 5.2.2
DMI (1 – n)	**Driver Machine Interface** At this point in time, this is the Driver Machine Interface (DMI) for all OCORA core CCS functions in need of user interaction. At a later stage, other functions may also be supported by the DMIs. The number of DMIs and the functions assigned to them can differ for the various implementations, depending on the RU's need. A typical OCORA implementation foresees one primary DMI for ETCS or the NTC system and an additional display for all other functions (e.g., ATO, Cabin Radio, etc.). In such configurations, the additional DMI may also be used to increase availability of the primary display functions through a switch-over mechanism. Mobile personal devices (e.g., Tablets) are another type of DMI that may be used for some applications.	▪ Chapter 5.2.3

Peripheral Devices		
Component	**High-Level Description**	**Link to Further Information**
MT (1 – n)	**Maintenance Terminal** The Maintenance Terminal (MT) is a laptop that can be connected to the CCN to perform maintenance tasks on all CCS On-Board components. Maintenance tasks should include the monitoring and downloading of diagnostic data, executing service commands (e.g., reboot of a specific component) and installing updates (new software, configuration, etc).	▪ Chapter 5.2.4
TRU (1 – n)	**Train Recording Unit** The Train Recording Unit (TRU) includes the Juridical Recording Unit (JRU) and the Diagnostic Recording Unit (DRU). Currently, the JRU is mostly located in the CCS domain while the DRU is typically found in the Train Control domain. The JRU records data from the ETCS system while the DRU is recording data from other On-Board systems, for instance the TCMS. In the future, other functions than ETCS will reside in the CCS domain (e.g., ATO). Those functions have also a need to record data. Hence, a DRU is proposed to be added to the CCS domain. Whether this is a specific hardware, in addition to the hardware available in the TCMS domain, or the DRU hardware can be combined needs to be explored further.	▪ Chapter 5.2.5
VL	**Vehicle Locator** The Vehicle Locator (VL) is a safe CCS On-Board component that uses sensor data and supporting information to provide train location output information safely and reliably. The Vehicle Locator (VL) is able to provide the absolute and relative position in reference to of the front end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles; hence, the VL is more than just an odometry component.	▪ Chapter 5.2.6
VLSs	**Vehicle Locator Sensors** The Vehicle Locator Sensors (VLS) provide raw data to determine speed, direction of travel, acceleration, position, and cold movement information to the Vehicle Locator. Depending on the RU's need and the progress of technology (e.g., GNSS, IMU) different type and quality of sensors may be used.	▪ Chapter 5.2.7
LTM	**Loop Transmission Module** The Loop Transmission Module (LTM) is used for ETCS L1 and L1LS systems to process the data from the Loop Transmission Antenna (LT-Antenna) and makes the data available on the CCN.	▪ Chapter 5.2.8
LT-Antenna	**Loop Transmission Antenna** The Loop Transmission Antenna (LT-Antenna) receives data through an RFID interface from the EURO Loop and provides the data to the Loop Transmission Module (LTM).	▪ Chapter 5.2.9
BTM	**Balise Transmission Module** The Balise Transmission Module (BTM) is used for ETCS L1 – L3 systems (inclu-ding L0 and LNTC). It processes the data from the Balise Transmission Antenna (BT-Antenna) and makes the data available on the CCN, for the ETCS application (VS). Optionally, the BTM can also receive data from KER Balises and make the data available, through the CCN, to the corresponding STM using the K interface described in SUBSET-101.	▪ Chapter 5.2.10
BT-Antenna	**Balise Transmission Antenna** The Balise Transmission Antenna (BT-Antenna) receives data through an RFID interface from the EURO Balise and provides the data to the Balise Transmission Module (BTM). Optionally, the BT-Antenna can also receive data through an RFID interface from the KER Balises and provide the data to the Balise Transmission Module (BTM).	▪ Chapter 5.2.11
STM	**Specific Transmission Module** The Specific Transmission Module (STM) represents the peripheral device implementing the STM functionality defined by the STM component of the NTC HW Solution (refer to 4.1.7).	▪ Chapter 5.2.12
NTC	**National Train Control** The National Train Control (NTC) represents the peripheral device implementing the NTC functionality defined by the NTC component of the NTC HW Solution (refer to 4.1.7).	▪ Chapter 5.2.13

Peripheral Devices		
Component	**High-Level Description**	**Link to Further Information**
NTC-Antennas	**National Train Control Antennas** The National Train Control Antennas (NTC-Antennas) receive the data from the trackside installations of the respective national ATP system and provides the data to the NTC.	▪ Chapter 5.2.14
PSs	**Perception Systems** The Perception System (PSs) provides awareness information if needed for GoA3 and GoA4 operations. In case of light signalling perception, the PSs may also be used for GoA1-2 operations. The Perception System processes the data from the various Perception Sensors (P Sensors), performs the necessary sensor fusion, and makes the data available on the CCN.	▪ Chapter 5.2.15
P-Sensors	**Perception Sensors** The Perception Sensors (P-Sensors) include all sensors to provide enough awareness of the environment (mainly the tracks) for safe GoA3 and GoA4 operations. In case of light signalling perception, the PSs may also be used for GoA1-2 operations. The sensors are mostly cameras, LIDAR and RADAR but can also include vibration sensors, smoke detectors, etc. (refer also to [14], Localisation On-Board – Introduction)	▪ Chapter 5.2.16
CVRL	**Cab Voice Radio Legacy** The CVRL is used for the communication between the driver and the operations control personnel and in some cases for communication between train staff. Today, it contains a control panel, a microphone, a loudspeaker, and a GSM-R voice radio and may connect directly with the PIS through a legacy connection (e.g., UIC) and to the DMI and/or JRU through respective connections. In current implementations, the CVRL is only loosely integrated into the CCS domain, if at all. But with the upcoming migration from GSM-R to FRMCS options become available to share the new connectivity infrastructure, the FRMCS On-Board System (5.3.1), between the CCS data and cabin voice.	▪ Chapter 5.2.17

Table 18 Peripheral devices

2.4.3 Connectivity devices

The connectivity devices are components outside the “OCORA Core” scope. For these components, OCORA only provides interface specifications, high-level functional requirements, and non-functional requirements. Basically, all requirements and specifications needed to ensure “plug & play”-like exchangeability. Of course, these specifications are only developed for the building blocks not already standardised (well enough) or where no standard is being developed by other organizations. The connectivity devices are also considered for all RAMSS aspects.

The connectivity devices provide secure connectivity to the data centres for the CCS On-Board domain. Eventually, other domains such as the train control or the passenger information may use this infrastructure for their communication needs. Refer to Appendix B for a discussion of possible options.

Connectivity Devices		
Component	**High-Level Description**	**Link to Further Information**
FRMCS On-Bord System	**FRMCS On-Board System** The FRMCS On-Board System implements the required functionalities and services providing the connectivity for the CCS Systems with the RBC (for ETCS L2/L3 networks), with ATO trackside (ATO-AT) and with the RCA compliant CCS Data Centres respectively. The FMRCS On-Board System runs on a dedicated hardware platform in a separate communication network to allow its services to be shared with other, non-CCS applications. This assures, that cybersecurity aspects are covered, and appropriate zoning models can be applied to the On-Board communication networks.	▪ Chapter 5.3.1
FRMCS Radio (1 – n)	**FRMCS Radio** The FRMCS Radio represents a modem with one or more 3GPP and/or non-3GPP radio access technologies supported by the FRMCS system.	▪ Chapter 5.3.2
GSM-R – EDOR	**GSM-R ETCS Data Only Radio** The GSM-R EDOR Radio provides (cyber-)secure GSM-R data connectivity to trackside systems. Today, it is mainly used for the communication with the RBC in case of ETCS level 2 operations. The device will become obsolete when FRMCS is rolled out on all trackside infrastructures.	▪ Chapter 5.3.3
MCG CCS	**Mobile Communication Gateway (CCS)** The Mobile Communication Gateway (MCG CCS) provides train to track-side connectivity for the On-Board CCS in case the trackside service is not available through FRMCS. Depending on the vehicle, it may also provide track-side connectivity for the systems (e.g., TCMS and PIS) of the Train Communication Networks.	▪ Chapter 5.3.4
Public Radio (1 – n)	**Public Radio** The Public Radio provides connectivity between the train and off-board. The OCORA architecture foresees that multiple Public Radio modems can be connected to the MCG CCS, depending on the RU’s need. Public Radio connections are mainly used for monitoring, diagnostic, and maintenance purposes during the transition phase to FRMCS. Separate modems can connect the train with the operations centre of its RU and/or with the train supplier. The Public Radio modem will eventually be replaced by the respective functionality of the FRMCS Radio.	▪ Chapter 5.3.5
Com Network	**Communication Network** The Communication Network is a standard IP network over Ethernet IEEE 802.3 where the communication systems (FRMCS On-Board System and MCG) for the trackside connectivity are attached. This separation from the other On-Board networks allows to apply appropriate zoning models addressing cybersecurity requirements.	▪ Chapter 5.3.6
Sec Network	**Security Network** The Security Network is a standard IP network over Ethernet IEEE 802.3 where the security systems for the On-Board Security Services (OSS) are attached. This separation from the other On-Board networks allows to apply appropriate zoning models addressing cybersecurity requirements.	▪ Chapter 5.3.7
Aux Network	**Auxiliary Network** The Auxiliary Network is a standard IP network over Ethernet IEEE 802.3 where the non-critical control components of the TCMS domain, the auxiliary components (e.g., toilets, climate and lighting) are located.	▪ Chapter 5.3.8

Connectivity Devices		
Component	**High-Level Description**	**Link to Further Information**
OSS	**On-Board Security Services** The On-Board Security Services encompasses the applications and services to assure cyber secure operations of the On-Board systems and networks.	▪ Chapter 5.3.9
Public Wi-Fi	**Public Wi-Fi** The Public Wi-Fi providing public Wi-Fi to the passengers of the train is not in the scope of the OCORA reference architecture. It is shown on the physical architecture to indicate the independence from any CCS On-Board system and network.	▪ Chapter 5.3.10

Table 19 Connectivity devices

3 Building block identification

Modularity with the purpose of having “plug & play”-like exchangeability as defined in the OCORA context (see red box below), requires very detailed interface descriptions as well as harmonized requirement specifications (functional and non-functional) for all building blocks. Defining these interfaces and requirements to the level needed for the OCORA desired “plug & play”-like exchangeability, requires a substantial deployment of scarce human resources. Therefore, the granularity of the decomposition needs to be a result of a well-balanced analysis of the effort against the business needs (expected benefits).

In order to limit these efforts for modularization and to provide to the supplier industry as much room as possible to re-use their current products, OCORA is not aiming at “plug & play”-like exchangeability for all components identified in chapter 2.3 and 2.4. Instead, components are combined in building blocks that need to fulfil the exchangeability criteria. The definition of a building block is as follows.

A building block is a top-level unit of the CCS On-Board system (hardware and/or software), having well defined capabilities (tasks to be performed to achieve a predefined result) and interfaces towards other building blocks of the CCS system. Building blocks consist of 1 – n component(s) and are regression free modifiable / adaptable and therefore portable / replaceable. As a result, every building block is “plug & play”-like exchangeable without impacting other building blocks. OCORA building blocks shall be an optimal balance between "number of interfaces between building blocks" and "desire to exchange building blocks at a low granularity".

While OCORA aims primarily for “plug & play”-like exchangeability at a building block level, exchangeability at a lower level is always welcome. This is facilitated using standardised COTS components within the building blocks. Therefore, OCORA strongly recommends to use / demand for standardised COTS components, wherever possible and reasonable.

The currently proposed decomposition into building blocks has been evaluated using the design principles as stated in the OCORA Guiding Principles [8], the OCORA Stakeholder-Requirements [25], in the OCORA Program-Requirements [26], and in the OCORA Design-Requirements [27].

Figure 7 depicts the currently proposed software building blocks and Figure 8 shows the proposed hardware building blocks. OCORA is aware that currently functionality (software) is dependent on certain hardware and separating hardware and software building blocks is hard to achieve. However, a separation of CCU hardware from software is envisioned by OCORA as outlined in chapter 9. As a result, there will be no dependency between CCU hardware and OCORA software anymore. The “Runtime Environment” (refer to chapter 9) acts as hardware abstraction and may be bundled with the hardware.

3.1 Software building blocks

OCORA aims at defining the interfaces between the software building blocks and the functional and non-functional requirements of each software building block. This standardization ensures "plug & play"-like exchangeability of every software building block. The currently proposed software building blocks are highlighted in Figure 7.

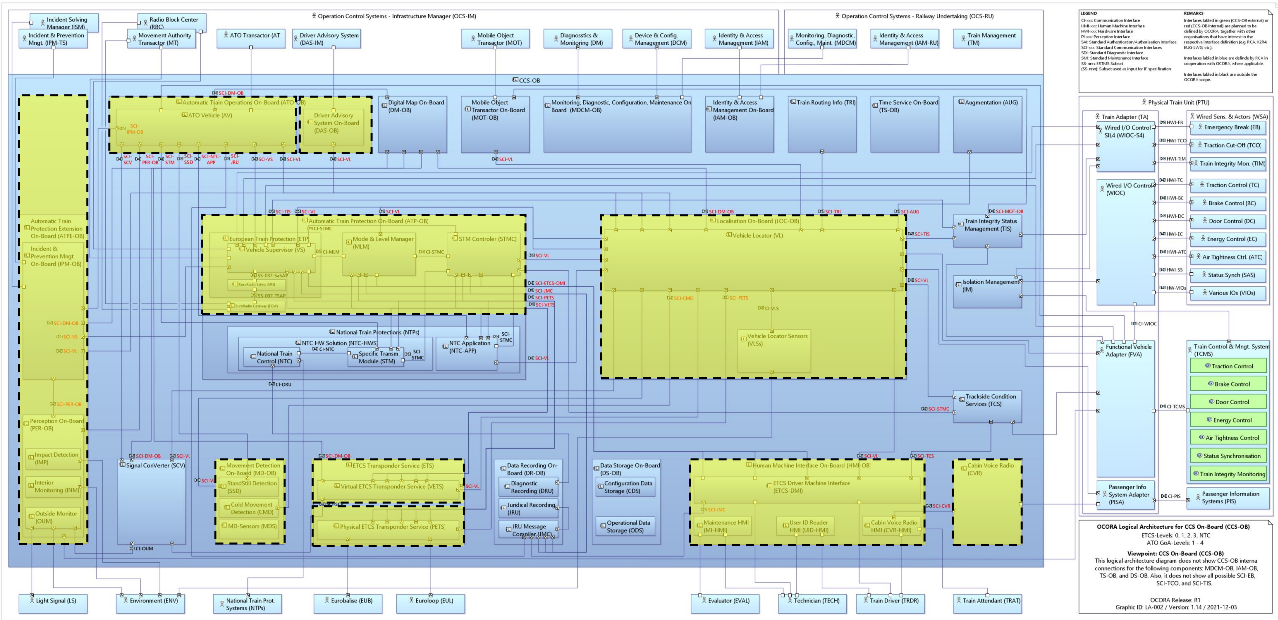

Figure 7 Software building blocks (tentative)

3.2 Hardware building blocks

OCORA also aims at defining the interfaces between the hardware building blocks and the functional and non-functional requirements of each hardware building block. This ensures "plug & play"-like exchangeability of every hardware building block. The currently proposed hardware building blocks are highlighted in Figure 8.

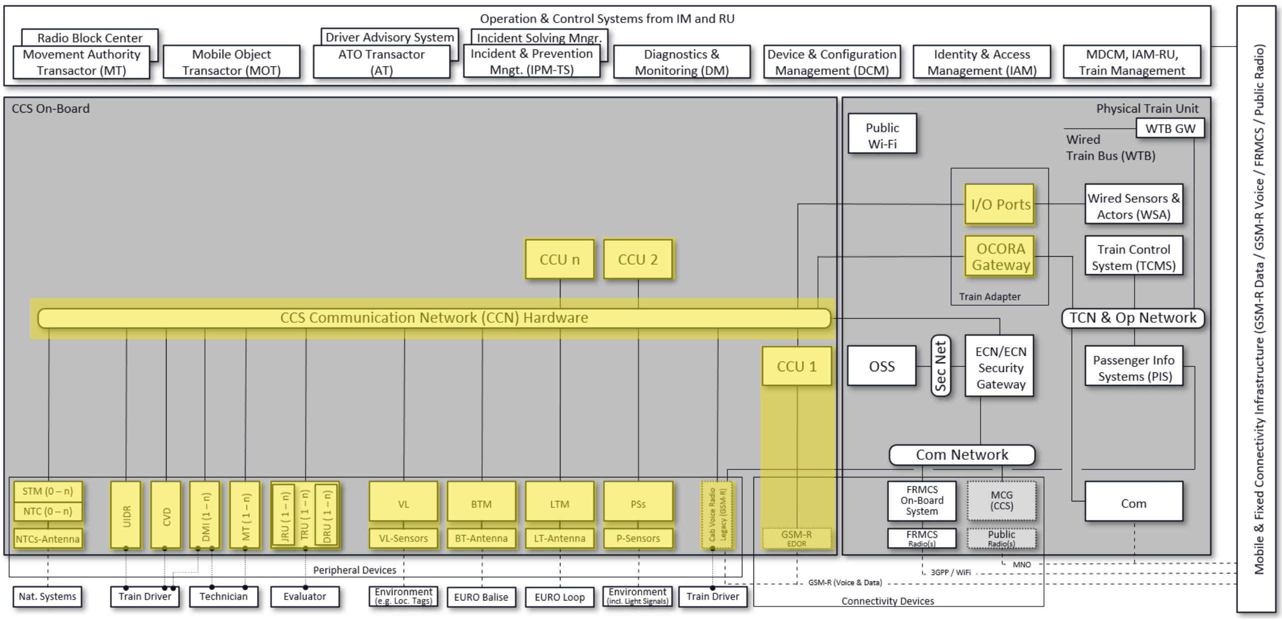

Figure 8 Hardware building blocks (tentative)

4 CCS-OB Logical architecture

The development of the OCORA System Architecture follows an iterative approach, evolving within the progress of the OCORA collaboration. With this release, OCORA made its first step towards using Model Based Systems Engineering (MBSE) based on the Arcadia methodology. Figure 9 depicts the currently defined OCORA logical architecture for the CCS On-Board.

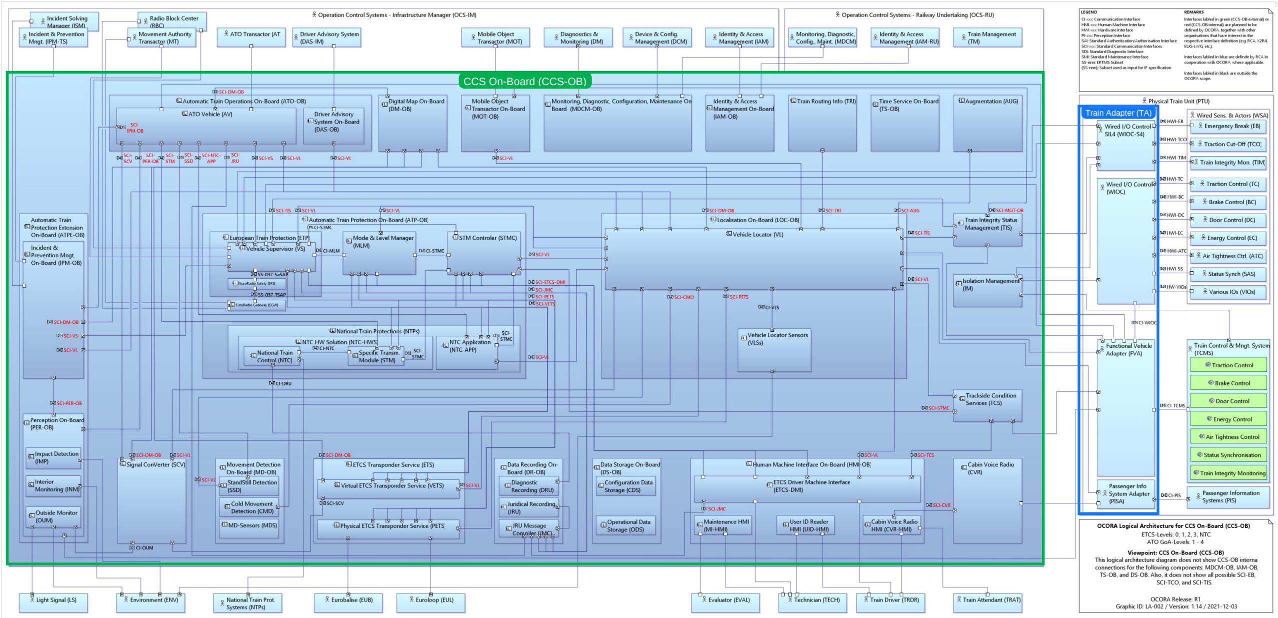

Figure 9 Logical architecture

(refer to Appendix D4 for large scale representation)

OCORA has started using the Capella MBSE tool for developing the logical architecture, well knowing that the Arcadia methodology proposes to start with the operational- and system-analysis before diving into the development of the logical architecture. It has been a deliberate decision to deviate from the Arcadia proposed approach:

1. The CCS On-Board system is considered a sub-system of the overall CCS system which includes CCS on-board and CCS trackside. OCORA favours the development of the operational- and system-analysis on a system and not on a sub-system level. This is to ensure the proper development of the end-to-end functionality and to minimize integration efforts at a later stage. The close collaboration with RCA (responsible for the overall CCS system architecture) for developing system capabilities has just started but OCORA aims to develop and communicate its ideas for the CCS On-Board in parallel. This can be done best through a high-level logical and physical architecture.

2. The CCS On-Board system is a well-known system that exists today and is already documented to a certain extent on a logical- and physical architectural level. Starting from this status quo architecture and applying the OCORA Guiding Principles [8], the OCORA Stakeholder-Requirements [25], the OCORA Program-Requirements [26], and the OCORA Design-Requirements [27] has dramatically accelerated the development of an initial versions of the OCORA System Architecture. The currently proposed logical and physical architecture will be iteratively adjusted and concluded once functions are being allocated to logical components (typically after completion of the system analysis phase). During the latter process, new logical components may evolve, some may be combined, and others may disappear entirely.

3. OCORA aims to develop its CCS On-Board architecture in close collaboration with other programs and sector initiatives (e.g., RCA, TOBA, EEIG ERTMS UG LWG, CONNECTA, LinX4Rail, X2Rail-4, UNISIG/UNIFE, etc.). Most of these programs have not yet performed and documented the operational- and systems-analysis but have developed a logical and/or physical architecture. To fit in the overall railway / CCS landscape and to facilitate understanding and communication between the different programs, OCORA adopts logical and physical components from other programs wherever reasonable. Adjustments will be performed iteratively at different points in time, concluding in a final logical architecture after completion of the functional allocation process.

Moving forward, OCORA plans to collaborate very closely with RCA and other programs in performing the system analysis and developing the system capabilities including functional chains and scenarios.

The currently proposed logical architecture is also and especially a result of the collaboration work with RCA, EUG-LWG and X2Rail-4. The alignment on the actors has reached quite a good level and alignment work on the logical components has started. The OCORA logical architecture will continue to evolve alongside with the developments in the mentioned programs.

4.1 Automatic Train Protection On-Board (ATP-OB)

The logical component ATP-OB includes the functionality needed for the automatic train protection. This includes the functionality of the European Train Protection (ETCS) as well as any functionality needed for National train Protection.

Figure 10 identifies the LCO-OB component in the overall CCS-OB architecture (yellow block) and depicts all interfaces to all currently know CCS-OB actors and CCS-OB components.

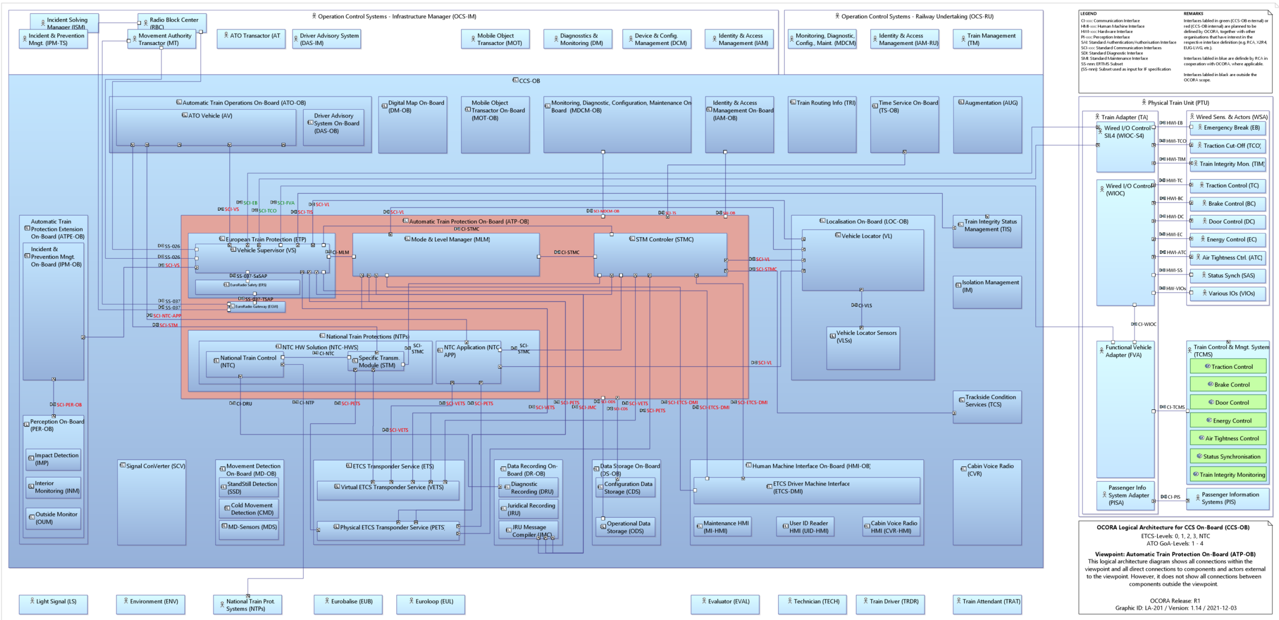

Figure 10 ATP-OB actors and external interfaces

(refer to Appendix D5 on page 114 for large scale representation)

4.1.1 European Train Protection (ETP)

The logical component ETP contains the VS functionality.

4.1.2 Vehicle Supervisor (VS)

The Vehicle Supervisor (VS) application, deployed on the OCORA computing platform, is a safe ETCS application (mandatory requirements are specified in SUBSET-026) in charge of calculating location specific speed limits (based on various inputs) and activating the braking system in case of speed limit overshoot. Location information is received from the Vehicle Locator (VL). In addition, information is received from the Balise Transmission Module (BTM) and the Loop Transmission Module (LTM) and processed adequately. In ETCS L2 and L3 mode, the VS interacts with the RBC or the APS-MT respectively. It receives the movement authority (MA) and reports the train position (TPR) to the respective system. The VS is agnostic to the communication technology used. Therefore, communication via GSM-R as well as via FRMCS or any future technology is possible. The VS also displays to the driver the necessary information (including cab signalling in ETCS L1, L2 and L3). It supports all ETCS modes and ETCS levels defined in the TSI-CCS.

The VS application is deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the VS component in the OCORA.

In today's ETCS implementations, the VS is part of the monolithic ETCS OBU. Since the VS is a safe application and is expected to have a very different technological life cycle than the VL, it is essential that the VS is a separate component, containing just the minimum functionality needed to perform the supervision of the vehicle during ETCS operations. Appendix C contains, on a very high-level, a first proposed split of functionality between the VS, VL, and the MLM / STMC, based on SUBSET-026, chapter 4.5. The OCORA architecture team is aware that splitting the functionality only based on the SUBSET-026, chapter 4.5 is not sufficient, because the subset does not provide all requirements. SUBSET-026 is providing the mandatory requirement specifications only. A more detailed separation and a first version of a VS model, identifying additional requirement to SUBSET-026, can be expected in subsequent OCORA documentation releases.

Isolating the VS- from the VL- and MLM- / STMC-functionality has the positive side-effect that the complexity of the VS is reduced and a stable component with little need for changes can be developed. A very important aspect since the VS is requiring a safe implementation and already many changes for the CCS On-Board are foreseeable. For example, it is expected that changes will be introduced, and more functionality will be added to CCS On-Board in the upcoming TSI-CCS revisions and through the introduction of new functionalities (game changers).

New functionalities (game changers) with potential impact on the VS are:

- FRMCS
- ATO
- Train integrity detection for ETCS L3 mode

It is the goal of the OCORA architecture team to build a VS model that is mostly agnostic to these changes, and where not possible, does already consider the changes in the design.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

The VS is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the VS component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.3 EuroRadio Protocol

To address the design principles of OCORA, the current EuroRadio Protocol as specified in SUBSET-037 needs to be divided into multiple parts allowing a split between safe-/ non-safe functionalities and to enable access to future mobile communication technologies such as FRMCS without changing the safe part of the upstream application (e.g., ATP-OB/ETCS).

Figure 11 below illustrates the allocation of the divided functionalities (Safe Functional Module and Communication Functional Module) onto the OCORA Safe Computing Platform.

The Vehicle Supervisor (VS) and the EuroRadio Safety Layer (ERS) as Part of the ATP-OB component run on multiple instances to provide the appropriate safety integrity level (SIL) to the overall system. The EuroRadio Gateway acts as the gateway between the Safe Computing Platform and the external, non-safe entities (e.g., On-Board FRMCS). The EuroRadio Gateway is also responsible for the coordination between the legacy EDOR and the new FRMCS On-Board System and implements the FRMCS client realizing the loose coupling to the services of the On-Board FRMCS.

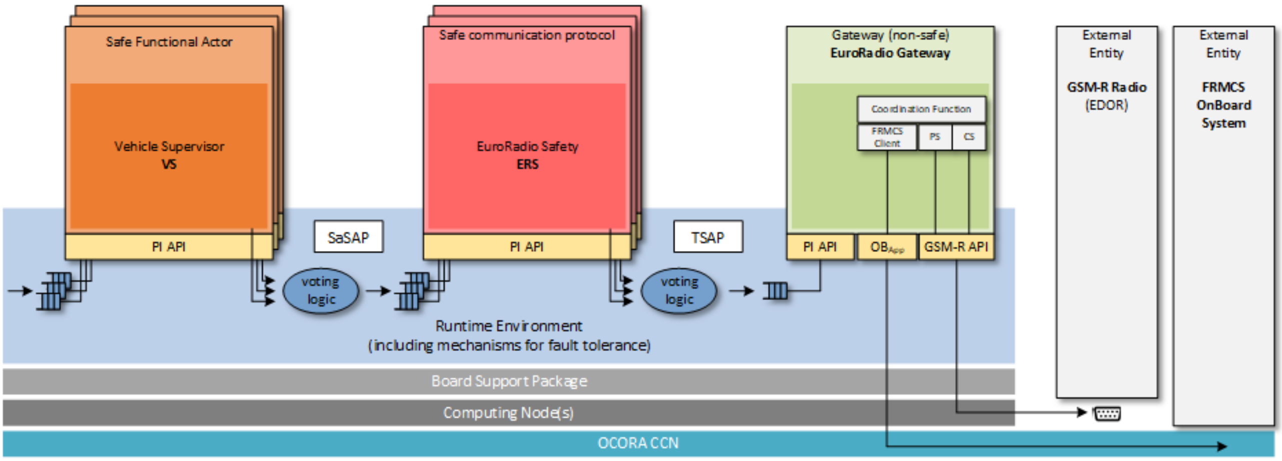

Figure 11 EuroRadio Safety allocation on the Safe Computing Platform

4.1.4 Mode and Level Manager (MLM)

The Mode & Level Manager (MLM) is a safe component of the ETCS Core in charge of managing the ETCS modes and levels. It ensures that the proper ETCS mode and level are active and manages the transitions from one mode or level to the other. In the latter context it also handles the handover between different RBCs. Furthermore, it makes sure that the correspondent information (e.g., current mode and level) is transmitted to the TCMS.

The MLM is deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the MLM component in the OCORA architecture. In today's ETCS implementations, the MLM is part of the monolithic ETCS OBU.

An analysis has been conducted in order to identify the information received and transmitted by the MLM. The result of the analysis is provided in document [16]. The methodology followed for the identification of input is based on the analysis of the SUBSET-026, chapter 4 (v3.6.0 incl. CR1238). The transition conditions provide the information needed by the MLM to compute mode and level state. We identify information already transmitted and specified in another logical component (FVA or HMI e.g.). The objective is to reuse information that are already defined. Document [16] contains multiple sheets:

- transition condition: each condition id in the SUBSET-026, chapter 4.6.3 table are made up of elementary condition which are repeated several times through the table.
- Each elementary condition is listed with:
  - condition where they are involved

- logical component which provides this information

- MLM IN: identify entry signal of the logical component. Elementary condition are state of an information (desk open / desk close are elementary condition of the information cabin status e.g.) An input signal contains one or several information (driver acknowledgment OS, SR, SH... e.g.). Information that are already defined are reused (FVA specification interface, subset 121 e.g.)
- MLM OUT: output of the MLM and identification of the recipient logical component
- MLM function: list of function supported by MLM
- Open Point: Point to be discussed for future evolution of the document

It is planned to complete the analysis for OCORA R 2 by adding the following information: trigger (time or event), time constraint, safety of information exchanged, identification of function which use the information in the MLM and functions which use the information in another logical component.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.5 STM Controller (STMC)

The STM Controller (STMC) is a safe component of the ETCS Core in charge of managing the safety authority between ETCS and installed national ATP systems (STM / NTC). It ensures that the proper ATP system is active and manages the switch-over from ETCS to the national ATP system and vice versa. The STMC interacts with the national ATP systems as defined in SUBSET-035 and SUBSET-058. The STMC with the respectively integrated national ATP systems enable an automatic transition from ETCS to the national ATP system and vice versa while the vehicle is driving.

The STMC is deployed on every OCORA based CCS On-Board system where a need for operating in national ATP systems exists. Refer to Appendix D4 on page 113 to locate the STMC component in the OCORA architecture. In today's ETCS implementations, the STMC is part of the monolithic ETCS OBU and corresponds to the STM Control Function defined in SUBSET-035.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.6 National Train Protections (NTPs)

The NTPs provides Automatic Train Protection functionality on national level. The NTPs can be either a dedicated NTC HW Solution (NTC-HWS) or it can be deployed as NTC Application (NTC-APP) running on the OCORA computing platform.

The NTPs is foreseen to be deployed on every OCORA based CCS On-Board system in need of NTP. Refer to Appendix D4 on page 113 to locate the NTPs component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.7 NTC HW Solution (NTC-HWS)

The NTC-HWS is a dedicated hardware solution implementing the national Automatic train protection solution with the NTC and STM components.

The NTC-HWS is foreseen to be deployed on every OCORA based CCS On-Board system in need of NTP. Refer to Appendix D4 on page 113 to locate the NTC-HWS component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.8 National Train Control (NTC)

The National Train Control (NTC) implements the national Automatic Train Protection functionality on dedicated hardware. It communicates with other OCORA components, namely the STM and can also use the functionality of other components connected to the CCN (e.g., DRU).

The NTC is foreseen to be deployed on every OCORA based CCS On-Board system in need of NTP. Refer to Appendix D4 on page 113 to locate the NTC component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.9 Specific Transition Module (STM)

The Specific Transmission Module (STM) provides the connection between the ETCS system (in case of OCORA the CCN) and the National Train Control System (NTC). The STM and the NTC are often closely integrated, hence the term STM is often used, when referring to the NTC system.

The STM is foreseen to be deployed on every OCORA based CCS On-Board system in need of NTP. Refer to Appendix D4 on page 113 to locate the STM component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.1.10 NTC Application (NTC-APP)

The National Train Controls Applications (NTC-APP), deployed on the OCORA computing platform, are safe applications in charge of ensuring Automatic train protection based on national systems. NTC-APPs, implemented on the OCORA computing platform, must communicate, as a minimum, with the Mode and Level Manager (MLM) and can use their specific sensors and actuators. In addition, they can take advantage of the standard OCORA interfaces. E.g., location information can be received from the Vehicle Locator (VL), data can be recorded in the DR-OB, DMI can be used, the TCMS can be accessed through the Functional Vehicle Adapter (FVA) and the NTC-APPs can also access balise telegrams through the ETCS Transponder Service (ETS) in order to get the packet 44 information.

Multiple NTC-APPs can be deployed on OCORA based CCS On-Board system, depending on the requirements of the rail network, the RU wants to operate in. Refer to Appendix D4 on page 113 to locate the NTC-APPs in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.2 Automatic Train Protection Extension On-Board (ATPE-OB)

This logical component includes all functionality needed for extending from ATO GoA 1-2 to ATO GoA 3-4.

4.2.1 Incident & Prevention Management On-Board (IPM-OB)

X2Rail-4 definition as per document [32]: This logical component is in the train and should substitute Train Driver and Train Attendant responsibilities for reacting in case of an incident (Incident and Prevention Management - Onboard). It manages safe reflexive reactions, computed reactions, and safety procedures in cooperation with IPM-TS and ISM.

The IPM-OB logical component is deployed on every OCORA based CCS On-Board system in need of ATO GoA 3 or GoA 4 functionality. In case of light signalling perception, the IPM-OB may also be used for GoA1-2 operations. Refer Appendix D4 on page 113 to locate the PER-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.2.2 Perception On-Board (PER-OB)

X2Rail-4 definition as per document [32]: The Perception (PER) component is in the train and senses the Physical Railway Environment in place of a driver.

The PER-OB logical component is deployed on every OCORA based CCS On-Board system in need of ATO GoA 3 or GoA 4 functionality. In case of light signalling perception, the PER-OB may also be used for GoA1-2 operations. Refer Appendix D4 on page 113 to locate the PER-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.2.3 Impact Detection (IMP)

The IMP detects impacts of the train with an object and informs the IPM-OB accordingly (refer also to RCA definition for "SubSys IMP" in document [30]).

The IMP logical component is deployed on every OCORA based CCS On-Board system in need of ATO GoA 3 or GoA 4 functionality. Refer Appendix D4 on page 113 to locate the IMP component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.2.4 Interior Monitoring (INM)

The INM monitors the environment inside the train and informs the IPM-OB about any abnormalities (refer also to RCA definition for "SubSys INT" in document [30]).

The IMP logical component is deployed on every OCORA based CCS On-Board system in need of ATO GoA 3 or GoA 4 functionality. Refer Appendix D4 on page 113 to locate the IMP component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation

4.2.5 Outside Monitoring (OUM)

OUM monitors the environment around the train and informs the IPM-OB about any abnormalities (refer also to RCA definition for "SubSys TFM" in document [30]).

The IMP logical component is deployed on every OCORA based CCS On-Board system in need of ATO GoA 3 or GoA 4 functionality. Refer Appendix D4 on page 113 to locate the IMP component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation

4.3 Localisation On-Board (LOC-OB)

The logical component LOC-OB contains the VL and VLS functionality.

Figure 12 identifies the LCO-OB component in the overall CCS-OB architecture (yellow block) and depicts all interfaces to all currently know CCS-OB actors and CCS-OB components.

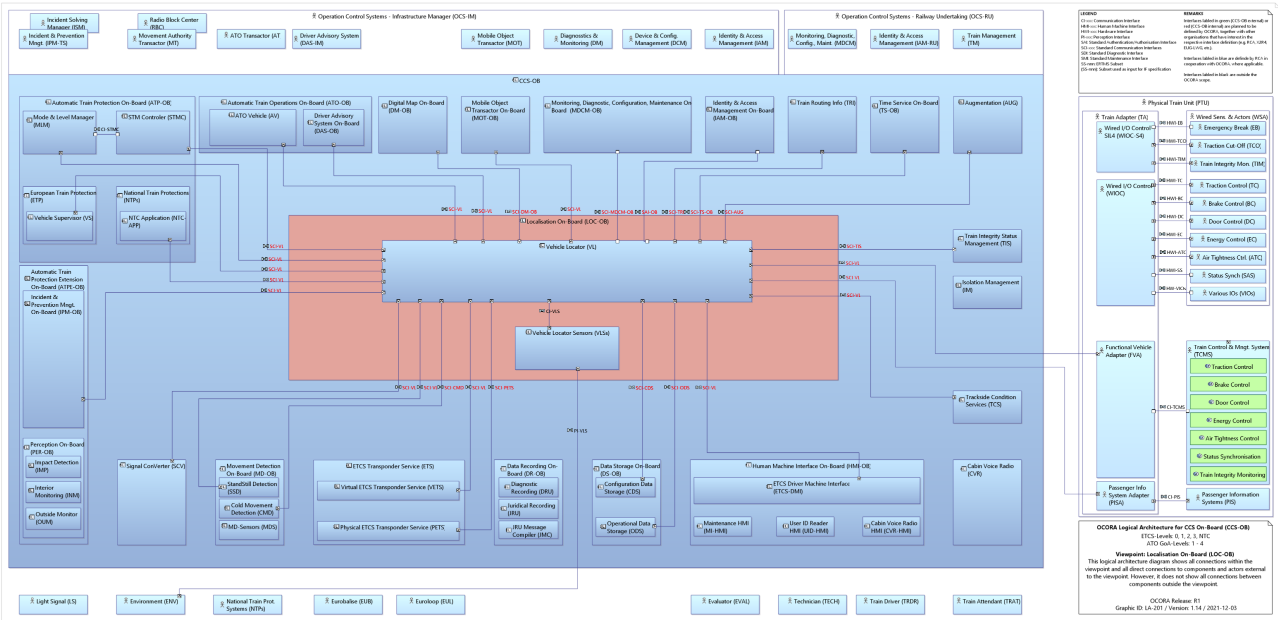

Figure 12 LOC-OB actors and external interfaces

(refer to Appendix D6 on page 115 for large scale representation)

4.3.1 Vehicle Locator (VL)

The Vehicle Locator (VL) is a safe CCS On-Board component that uses sensor data and supporting information to provide train location output information safely and reliably. The Vehicle Locator (VL) is able to provide the absolute and relative position of the front end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles; hence, the VL is more than just an odometry component.

The VL is deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the VL component in the OCORA architecture.

In today's ETCS implementations, the VL is part of the monolithic ETCS OBU. Since the VL has a different technological life cycle than the VS, it is essential that the VL is a separate component, containing just the functionality needed to perform the vehicle localisation. This allows new localization technologies to be introduced more quickly in the future without the need to modify the VS functionality. Appendix C contains, on a very high-level, a first proposed split of functionality between the VS, and VL, based on SUBSET-026, chapter 4.5. The OCORA architecture team is aware that splitting the functionality only based on the SUBSET-026, chapter 4.5 is not sufficient, because the subset does not provide all requirements. SUBSET-026 is providing the mandatory requirement specifications only. A more detailed separation and a first version of a VL model, identifying additional requirements to SUBSET-026, can be expected in subsequent OCORA documentation releases.

Isolating the VL- from the VS-functionality has the positive effect that the complexity of the VL is reduced. A very important aspect, since the VL is requiring a safe implementation and already many changes for the CCS on-board, impacting the VL, are foreseeable. New functionalities (game changers) with potential impact on the VL are:

- FRMCS
- ATO
- Train integrity detection for ETCS L3
- GNSS augmentation
- Digital map

It is the goal of the OCORA architecture team to build a VL model that is mostly agnostic to these changes, and where not possible, does already consider the upcoming changes in the design.

Further details can be found in document [14] and [15].

4.3.2 Vehicle Locator Sensors (VLS)

This logical component includes the functionality the locator sensors are providing.

Further details can be found in document [14].

4.4 Automatic Train Operations On-Board (ATO-OB)

This logical component includes all functionality needed for ATO GoA 1-2.

4.4.1 ATO Vehicle (AV)

The ATO Vehicle (AV) application, deployed on the OCORA computing platform, is a non-safe application for Automatic train operations. A safe extension is needed for GoA3 and GoA4 operations. This is provided by the Automatic Train Protection Extension On-Board (ATPE-OB). The AV in GoA2 – GoA4 controls the vehicle's speed, using information received through the interface SS126. It also communicates with the Vehicle Supervisor (VS) over the interface SS130 (between AV and ETCS Core). Remark: AV is called ATO-OB in GoA2 Shift2Rail SUBSET-125.

The AV application is deployed on every OCORA based CCS On-Board system in need of ATO functionality. Refer to Appendix D4 on page 113 to locate the AV component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.4.2 Driver Advisory System On-Board (DAS-OB)

The Driver Advisory System On-Board is an optional and non-safe application calculating an energy efficient speed profile to achieve the pre-planned and dynamically updated train timings. It generates detailed driver advice for adhering to the planned timings while driving energy efficient. The trackside Driver Advisory System (DAS-IM) or the Traffic Management System (TMS) is responsible for conflict detection and calculation of new target train timings, that are forwarded to the DAS-OB and evaluated accordingly. The typical integration of DAS-OB application is defined EN 15380-4. The DAS-OB can also operate standalone (e.g., without integration into the vehicle). The DAS-OB is not needed if ATO Vehicle (AV) is installed, since the AV already includes the DAS functionality. The implementation of DAS application on the OCORA computing platform is an open issue to be solved in subsequent versions of this document (unsafe information displayed on the driver DMI). The DAV application can be deployed on OCORA based CCS On-Board system, depending on the requirements of the rail network, the RU wants to operate in. Refer to Appendix D4 on page 113 to locate the DAV component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.5 Digital Map On-Board (DM-OB)

The logical component DM-OB is a safe service deployed on the OCORA computing platform. The DM-OB provides topology and topography data (a.k.a. map data) that are certified for the usage in safety-relevant On-Board applications / services (e.g., VL, VS, PER-OB) up to SIL4. The service guarantees that the map data fulfils the quality criteria stated by trackside, e.g., accurate, precise, reliable, complete, and up-to-date map data. The DM-OB uses its own On-Board data storage that is updated, if required, using the functionality of the Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB) to propagate trackside map data (e.g., from Topo4) to the On-Board data storage.

The DM-OB is foreseen to be deployed on every OCORA based CCS On-Board system in need of GoA3 – GoA4 functionality or if the VL has a need for it. In case of light signalling perception, the DM-OB may also be used for GoA1-2 operations. Refer to Appendix D4 on page 113 to locate the DM-OB component in the OCORA architecture.

Examples of possible digital map objects/attributes are (with reference to the RCA topology concept): track edge, track node, track edge point (balise, track radius, gradient, cant, speed profile marker), and track edge section (tunnel, platform edge).

Example of service usage: The Vehicle Locator (VL) service uses the digital map service (DM-OB) to place sensor measurements into a common reference frame such that this data can be interlinked as part of a fusion algorithm. For example, a position determined by balise and relative path measurement (odometer) is georeferenced and fused with an absolute GNSS position before being mapped back to a position on the track edge to improve the accuracy and confidence of the actual train position.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.6 Mobile-Object Transactor On-Board (MOT-OB)

The logical component MOT-OB communicates with various CCS On-Board logical components and communicates with the MOT.

The MOT-OB is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the MOT-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.7 Monitoring, Diagnostic. Configuration, Maintenance On-Board (MDCM-OB)

The logical component MDCM-OB deployed on the OCORA computing platform, collects data relevant for local (through the Maintenance Terminal or DMI) and remote diagnostic and monitoring. For local maintenance, it provides the relevant data upon request to the Maintenance Terminal or DMI in a standardised format. For remote diagnostics and monitoring the data can be sent to multiple recipients (e.g., the RU of the vehicle, the IM the vehicle currently operates in, the vehicle provider, the CCS On-Board provider etc.). The owner of the vehicle can define in the vehicle's configuration (refer to Configuration Data Storage) what data is forwarded to which recipient(s).

The MDCM-OB is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the MDCM-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.8 Identity & Access Management On-Board (IAM-OB)

The Identity & Access Management On-Board (IAM-OB) is a service deployed on the OCORA computing platform. It integrates with the IAM System providing the central management for the identification, authentication and authorisation of devices and applications to resources and functions of the CCS On-Board and trackside systems. For the identification, the IAM System manages a unique ID for each entity (e.g., device, application). The granularity, on what level the system will be split into separate entities is not yet defined. It can reach from one single ID for the overall CCS On-Board system to IDs for any single device connected to the CCN and to application, running on the OCORA Platform. For the authentication of a device or an application, the solution could be based on the Public Key Infrastructure (PKI) or Message Authentication Codes (MAC) using symmetrical encryption mechanisms like 3DES or AES. The access to resources and functions is centrally managed by roles and granted on a Need-to-Know principle to limit unauthorised access to resources and functions within the CCS On-Board system.

The IAM-OB is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the IAM-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.9 Train Routing Info (TRI)

An interlocked (safe) train path uniquely assigned to a train/vehicle. This information is seen useful to validate the determined position by the Vehicle Locator (VL) against track selectivity.

The TRI is foreseen to be deployed on every OCORA based CCS On-Board system in need of track selectivity. Refer to Appendix D4 on page 113 to locate the TRI component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.10 Time Services On-Board (TS-OB)

The Time Service On-Board (TS-OB) provides a service that allows all On-Board components to have their time in synch with a master clock and therefore in synch with each other and the trackside systems (e.g., safe data centres). The time base is assumed to be UTC and components in need to display the time can convert it to local time based on the systems time zone settings. The TS-OB functionality is significant to simplify diagnostic and analysis tasks and is important for ATO operations, and other aspects (e.g., used to timestamp the output of the localisation system with the validity time of the information provided).

The TS-OB is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the TS-OB component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.11 Augmentation (AUG)

Augmentation of a positioning system is a method of improving – "augmenting" - the positioning system's performances, such as integrity, accuracy, or availability thanks to the use of external information. (source EUG-S2R JWG).

There is the possibility to acquire the augmentation data through the GNSS receiver (sensor). But this approach is expected to have availability limitations not acceptable in the rail environment. Therefore, discussions are currently ongoing to provide augmentation data through decentralised stations through the connectivity network (GSM-R, FRMCS).

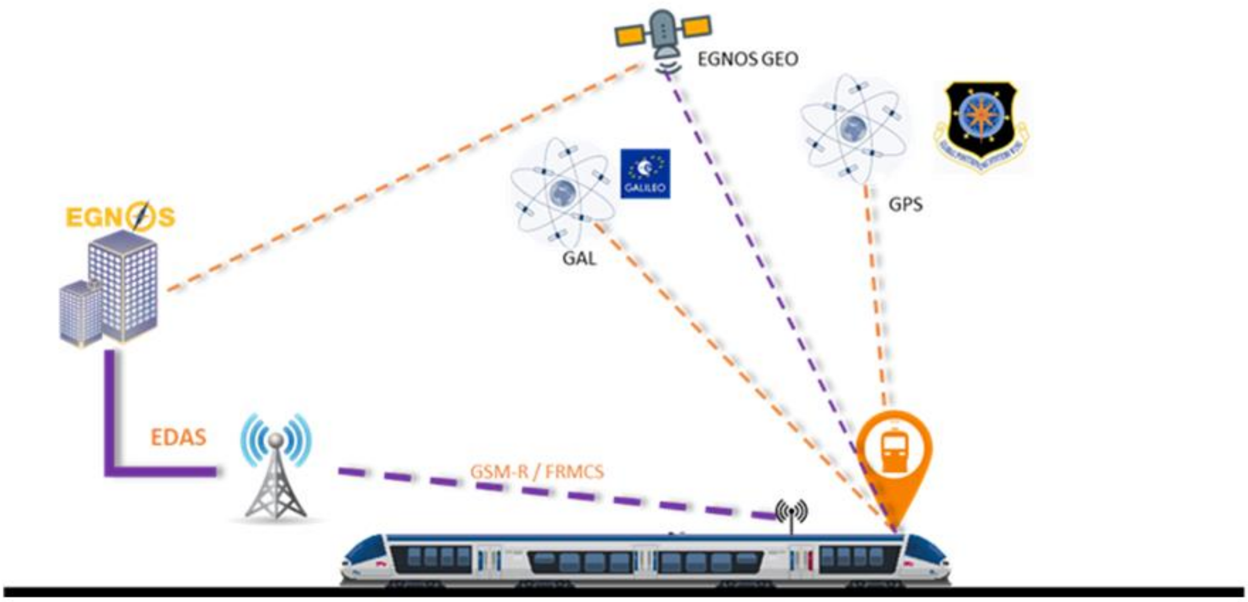

Figure 13 Augmenting GNSS position data

4.12 Train Integrity Status Management (TIS)

The Train Integrity Status Management is a safe component deployed on the OCORA computing platform or the OCORA gateway. It provides the train integrity status in a standardised fashion to the OCORA software components. To provide the train's integrity status, multiple options are possible:

a) train integrity determination on the train (e.g., through the TCMS),

b) second localisation unit at the end of the train with On-Board determination of the train integrity, and

c) second localisation unit at the end of the train with trackside determination of the train integrity.

The TIS component ensures that all CCS applications that need to know the train's integrity status (including the coupler statuses, if applicable) are receiving the information through a standardised interface, independent of the option used. The train integrity status also includes the total safe train length (including the safe length over coupled compositions).

4.13 Isolation Management (IM)

The logical component IM allows to isolate one or multiple ATP systems and informs the PTU accordingly.

4.14 Trackside Condition Services (TCS)

The Trackside Condition Services (TCS) is a non-safe component of the ETCS Core in charge of managing the trackside condition information received from balises, RIU, or RBC. It calculates the remaining distance to specific trackside points and triggers the appropriate actions according to the location. Location information is received from the Vehicle Locator (VL). Also, the TCS informs the driver about the trackside points: it sends the commands to display the different pictograms on the DMI depending on the trackside point and the relative location to it. Furthermore, it makes sure that the correspondent information is transmitted using the SCI-FVA interface via FVA to the vehicle, and the distance information is updated as needed. The TCS remains active during level transitions, including transition to level NTC.

The TCS component is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the TCS component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.15 Cabin Voice Radio (CVR)

The logical component CVR, deployed on the OCORA computing platform, implements the Cab Voice Radio functionality. The CVR is operated through the CVR-HMI component, which allows the train driver to initiate and receive voice communication between the train and the trackside operations control centres. In some cases, the CVR may also provide the functionalities to communicate with the train staff and to use the Passenger Information System for announcements by using the SCI-PISA interface.

For communication with the trackside operation control centres, the CVR component is using the services provided by the FRMCS On-Board System.

The CVR application can be deployed on OCORA based CCS On-Board system, once an FRMCS On-Board System is installed on the vehicle and FRMCS is rolled out on the infrastructure where the vehicle is used.

Refer to Appendix D4 on page 113 to locate the CVR component in the OCORA architecture.

In case GSM-R Radio is still used on the trackside infrastructure, the vehicle needs to be equipped with a legacy peripheral Cab Voice Radio (refer to 5.2.17) with a dedicated GSM-R radio module.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.16 Human Machine Interface On-Board (HMI-OB)

The logical component HMI-OB includes the functionality needed for any user interaction with the CCS On-Board. This includes the functionality to operate the European Train Protection (ETCS), the Cabin Voice Radio (CVR) as well as any functionality needed for local diagnostics and maintenance of the CCS On-Board.

4.16.1 ETCS Driver Machine Interface (ETCS-DMI)

The ETCS-DMI component provides the functionality for any user interaction with the ETCS On-Board system.

4.16.2 Maintenance HMI (MI-HMI)

The MI-HMI component provides the functionality for any user interaction regarding the maintenance of the CCS On-Board.

4.16.3 User ID Reader HMI (UID-HMI)

The UID-HMI component provides the functionality for any user interaction UID Reader off the CCS On-Board.

4.16.4 Cabin Voice Radio HMI (CVR-HMI)

The CVR-HMI component provides the functionality for any user interaction with the OCORA based Cab Voice Radio.

4.17 Data Storage On-Board (DS-OB)

The logical component DS-OB provides the functionalities to store and retrieve operational and configuration data used by the CCS On-Board.

4.17.1 Configuration Data Storage (CDS)

The Configuration Data Storage (CDS) stores static and semi-static data needed for the CCS On-Board system. The data storage is separated from the operational data and it is separated from the ETCS components (e.g., VS) to make the data easily available to other applications that may need it (e.g., VL). The Configuration Data Storage contains data provided when commissioning a CCS On-Board system for the first time and is changed whenever configurations of the vehicle change (e.g., additional sensors, additional DMI, etc.). The data is entered by service technicians through the local maintenance terminal or via the remote maintenance. In both cases this occurs through the Monitoring, Diagnostic, Configuration, Maintenance (MDCM-OB) component. In subsequent versions of the OCORA specifications, the CDS will be specified in detail.

The CDS component is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the CDS component in the OCORA architecture.

The ETCS On-Board application should implement configuration capability for the train characteristics, the latter being independent from other configuration parameters. This in order to allow defining the train characteristics for different train types without affecting the certification of the whole ETCS On-Board application, the same also being valid in case of modifications.

Scope of OCORA is to reduce the variability of implementation of the CCS On-Board applications (i.e. ETCS On-Board application). This is achieved by properly defining what is expected from the ETCS On-Board application in terms of configurability (at the end this results in a list of requested configuration parameters).

Goal is that CCS On-Board applications from different suppliers can be exchanged between each other, but also that the same CCS On-Board application can be deployed on different train types with a minimal effort.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.17.2 Operational Data Storage (ODS)

The Operational Data Storage (ODS) is a data storage for saving quite dynamic data that is entered / provided during an operational day of a vehicle and has no relevance for long-time safeguarding. The operational data storage is separated from the ETCS components (e.g., VS) to make the data easily available to other applications that may need it (e.g., ATO Vehicle). The operational data storage contains data provided by the driver, the TCMS, I/O Ports, and possibly the device and configuration management. Examples of Operational Data is the driver id, the train running number, the status of a cab, etc. In subsequent versions of the OCORA specifications, the ODS will be specified in detail.

The ODS component is foreseen to be deployed on every OCORA based CCS On-Board system. Refer to Appendix D4 on page 113 to locate the ODS component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.18 Data Recording On-Board (DR-OB)

The logical component DR-OB includes the Juridical Recording Unit (JRU), the Diagnostic Recording Unit (DRU) and the JRU Message Compiler (JMC). Currently, the JRU is mostly located in the CCS domain while the DRU is typically found in the Train Control domain. The JRU records data from the ETCS system while the DRU is recording data from other On-Board systems, for instance the TCMS. In the future, other functions than ETCS will reside in the CCS domain (e.g., ATO). Those functions have also a need to record data. Hence, a DRU is proposed to be added to the CCS domain.

4.18.1 Diagnostic Recording (DRU)

The DRU provides data recording mechanisms to applications residing in the CCS On-Board domain. Whether this is a specific hardware, in addition to the hardware available in the TCMS domain, or the DRU hardware can be combined needs to be explored further.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.18.2 Juridical Recording (JRU)

The JRU is recording data from the ETCS system.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.18.3 JRU Message Compiler (JMC)

The JMC aggregates data from the JRU and compiles them into a human readable format to support efficient data analysis.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

4.19 ETCS Transponder Service (ETS)

The logical component ETS provides real and/or virtual ETCS transponder messages to the CCS On-Board applications.

4.19.1 Virtual ETCS Transponder Service (VETS)

The VETS component generates virtual ETCS telegrams based on the current location using the Digital Map On-Board (DM-OB).

4.19.2 Physical ETCS Transponder Service (PETS)

The PETS component reads the ETCS telegrams from the trackside installed infrastructure (Eurobalise and Euroloop) and forwards them to the CCS On-Board applications.

4.20 Movement Detection On-Board (MD-OB)

The logical component MD contains the logical components SSD, CMD and MD-Sensors. It provides movement information to various consumers.

4.20.1 Stand Still Detection (SSD)

The logical component SSD is a vehicle-based function that detects if the train is standing still. Depending on the consumer of this information, different levels of stand-still thresholds may apply.

Remark from discussions with RCA: The SSD information is needed by the RCA-APS and must be provided by the vehicle. An example is the flank protection. It may be useful that a parked vehicle provides flank protection. The RCS-APS would need to know whether or not a vehicle is parked (SSD signal). There might be other scenarios where SSD information is needed/useful for RCA-APS (some of them already exist today). But for those scenarios it is not sufficient to report v=0, since this information is currently only reported in a resolution of 5 km/h, but RCA-APS would need to have a confirmed v=0 (performance and SIL-level currently unknown).

4.20.2 Cold Movement Detection (CMD)

The logical component CMD is a vehicle-based function that detects if the train has moved while the CCS-OB system was powered-off. The CMD function is especially needed in the migration phase. In the final phase, where the vehicle is "always on" and "always connected / located", the function may not be needed anymore.

It is under discussion, if CMD should also provide the magnitude of the cold movement (see also CR1345 – Threshold small movements). With the implementation of CR1350 (always connected, always reporting) CMD functionality on the vehicle may not be required anymore.

4.20.3 MD-Sensors (MDS)

The logical component MDS includes the functionality the movement detection sensors are providing.

4.21 Signal Converter (SCV)

The Signal Converter (SCV) is in the train and converts the information coming from optical signals into SUBSET-026 compliant information (refer also to X2Rail-4 definition as per document [32]).

5 CCS-OB Physical architecture

The development of the OCORA System Architecture follows an iterative approach, evolving within the progress of the OCORA collaboration. Figure 14 depicts the currently defined OCORA physical architecture for the CCS On-Board.

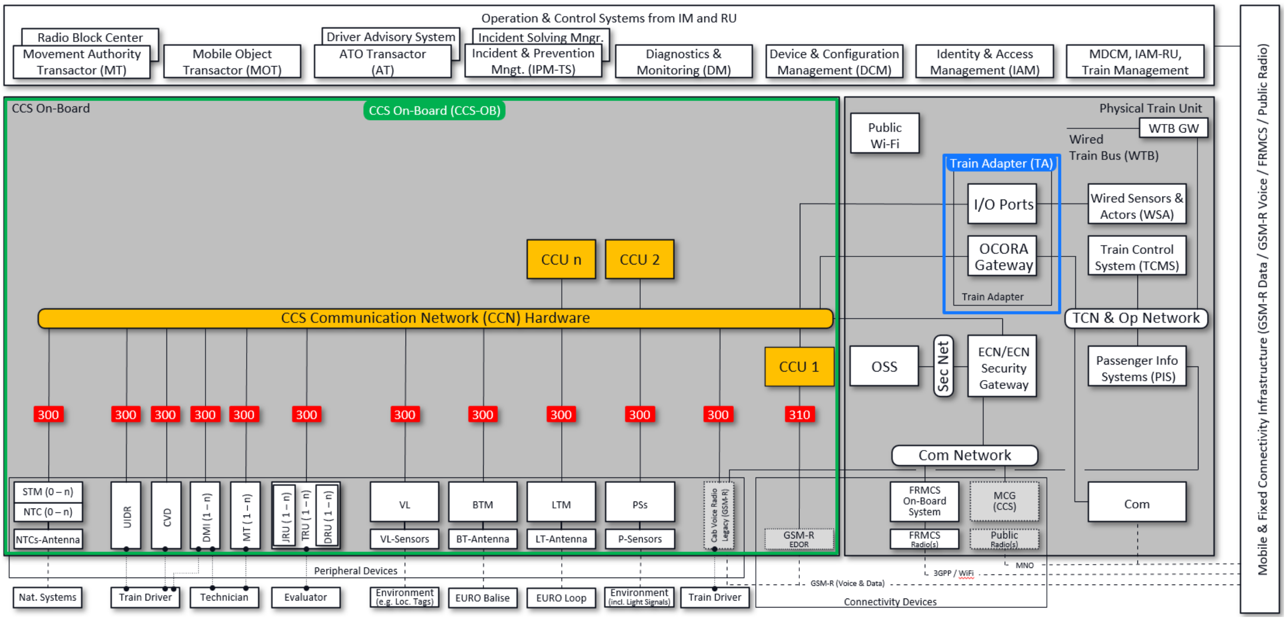

Figure 14 Physical architecture

(refer to Appendix D2 for large scale representation)

OCORA has started developing a physical architecture, well knowing that the Arcadia methodology proposes to start with the operational- and system-analysis before diving into the development of the logical and physical architecture. It has been a deliberate decision to deviate from the Arcadia proposed approach:

1. The CCS On-Board system is considered a sub-system of the overall CCS system which includes CCS on-board and CCS trackside. OCORA favours the development of the operational- and system-analysis on a system and not on a sub-system level. This is to ensure the proper development of the end-to-end functionality and to minimize integration efforts at a later stage. The close collaboration with RCA (responsible for the overall CCS system architecture) for developing system capabilities has just started but OCORA aims to develop and communicate its ideas for the CCS On-Board in parallel. This can be done best through a high-level logical and physical architecture.

2. The CCS On-Board system is a well-known system that exists today and is already documented to a certain extent on a logical- and physical architectural level. Starting from this status quo architecture and applying the OCORA Guiding Principles [8], the OCORA Stakeholder-Requirements [25], the OCORA Program-Requirements [26], and the OCORA Design-Requirements [27] has dramatically accelerated the development of an initial versions of the OCORA System Architecture. The currently proposed logical and physical architecture will be iteratively adjusted and concluded once functions are being allocated to logical components (typically after completion of the system analysis phase). During the latter process, new logical components may evolve, some may be combined, and others may disappear entirely.

3. OCORA aims to develop its CCS On-Board architecture in close collaboration with other programs and sector initiatives (e.g., RCA, TOBA, EEIG ERTMS UG LWG, CONNECTA, LinX4Rail, X2Rail-4, UNISIG/UNIFE, etc.). Most of these programs have not yet performed and documented the operational- and systems-analysis but have developed a logical and/or physical architecture. To fit in the overall railway / CCS landscape and to facilitate understanding and communication between the different programs, OCORA adopts logical and physical components from other programs wherever reasonable. Adjustments will be performed iteratively at different points in time, concluding in a final logical architecture after completion of the functional allocation process.

The currently proposed physical architecture is a result of the collaboration work with UIC TOBA regarding connectivity and S2R CONNECTA regarding on-board communication. The OCORA physical architecture will continue to evolve alongside with the developments in those programs and incorporate changes due to the advancing logical architecture.

The allocation of logical components to hardware is one of the last steps in the Arcadia methodology and will be performed by OCORA once the functional allocation to logical components is concluded. During that process new physical components may evolve, some may be combined, and others may disappear entirely.

5.1 OCORA core hardware

The OCORA core hardware are the components fully filled in orange. The OCORA core hardware, together with the runtime environment (refer to chapter 9), provides the platform to run the OCORA core functionality.

5.1.1 CCS Communication Network (CCN)

The CCS Communication Network (CCN) allows direct communication between all CCS On-Board components connected to it and eventually with external systems, such as the TCMS. The CCN is the most central part of the OCORA architecture and is the basis for achieving modularity that results in "plug & play"-like exchangeability of all identified building blocks. The CCN is a TSN Ethernet based network with the use of SDTv2/v4 as safety layer. On session layer (OSI layer 5, refer to OCORA OSI definitions in document [10]) different protocols (e.g., TRDP 2.0, OPC UA PubSub over TSN, DDS/RTPS over TSN) are possible. At the final stage, the CCN will be specified on all layers together with Shift2Rail CONNECTA/Safe4RAIL projects in the new IEC 61375 standards series. Refer to document [17] and Appendix B for further details (e.g., the network topology scenarios that OCORA considers for implementing the CCN).

The CCN is installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the CCN component in the OCORA architecture.

Every CCS On-Board device with high RAMS requirements has two TSN capable Ethernet ports. Refer to Appendix B for network topology scenarios.

Information regarding the requirements used for evaluating the CCN and the respective evaluation can be found in document [17].

5.1.2 CCS Computing Unit (CCU)

The CCS Computing Unit (CCU) is the computing hardware for all OCORA core CCS functions. One CCU can contain multiple processor boards (e.g., to provide hardware level voting). The number and the functional behaviour of the CCUs can differ for the various implementations, depending on the RU's need. For migration reasons, multiple CCUs may be needed, or certain functions can be deployed on one node (e.g., safe functions) while others (e.g., non-safe) are deployed on a separate node. In some projects, additional CCUs may be used to increase availability and reliability by defining one or multiple CCU nodes as fail over or standby units. The CCU hardware is made accessible through the runtime environment. The CCU together with the runtime environment are building the computing platform (refer to chapter 9 for details).

At least one CCU is installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the CCU component in the OCORA architecture.

Further details regarding the CCU hardware will be provided in subsequent versions of the OCORA architecture documentation.

5.2 Peripheral devices

The peripheral devices are components outside the "OCORA Core" scope. For these components, OCORA provides interface specifications, high-level functional requirements, and non-functional requirements only. Basically, all requirements and specifications needed to ensure "plug & play"-like exchangeability. Of course, these specifications are only developed for the building blocks not already standardised (well enough) or where no standard is being developed by other organizations. The peripheral devices are also considered for all RAMSS aspects.

The peripheral devices include all sensors and actuators needed for the CCS On-Board system to function and to be able to perform the necessary maintenance tasks.

5.2.1 User Identification Reader (UIDR)

The User Identification Reader (UIDR) is used to automate the identification pro cess for drivers and service technicians. RFID card readers may be the most common option used at this point in time. But as technology advances, fingerprint, face ID, etc. might become viable options. The OCORA specifications will be technology agnostic.

The UIDR is an optional deployment on OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the UIDR component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.2 Cabin Voice Device (CVD)

The Cabin Voice Devices (CVDs) are the handset, the microphone and the loudspeaker(s) in the cabin, combined with some electronics, allowing to communicate over the CCN with the CVoIP application and ultimately with the FRMCS On-Board System. They are used for the communication between the driver and the operations control personnel or for communication between train staff. Today, these devices are part of a dedicated Cabin Voice Radio and are only loosely integrated into the CCS domain, if at all. But with the upcoming migration from GSM-R to FRMCS options become available to share the new connectivity infrastructure between the CCS data and cabin voice. The OCORA concept foresees to have a cabin voice application running on one of the CCUs and providing voice communication through voice over IP (VoIP).

The CVDs are an optional deployment on OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the CVD components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.3 Driver Machine Interface (DMI)

At this point in time, this is the Driver Machine Interface (DMI) for all OCORA core CCS functions in need of user interaction. At a later stage, other functions may also be supported by the DMIs. The number of DMIs and the functions assigned to them can differ for the various implementations, depending on the RU's need. A typical OCORA implementation foresees one primary DMI for ETCS or the NTC system and an additional display for all other functions (e.g., ATO, Cabin Radio, etc.). In such configurations, the additional DMI may also be used to increase availability of the primary display functions through a switch-over mechanism. Mobile personal devices (e.g., Tablets) are another type of DMI that may be used for some applications.

At least one DMI is installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the DMI components in the OCORA architecture.

OCORA plans to build on top of the European Driver's Desk (EUDD) specification work when developing the OCORA DMI interface specifications. It is an aim of OCORA to support a better interchangeability of the DMIs, than in the present market scenario.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.4 Maintenance Terminal (MT)

The Maintenance Terminal (MT) is a laptop that can be connected to the CCN to perform maintenance tasks on all CCS On-Board components. Maintenance tasks should include the monitoring and downloading of diagnostic data, executing service commands (e.g., reboot of a specific component) and installing updates (new software, configuration, etc).

Multiple MTs can be connected to every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the MT components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.5 Train Recording Unit (TRU)

The Train Recording Unit (TRU) includes the Juridical Recording Unit (JRU) and the Diagnostic Recording Unit (DRU). Currently, the JRU is mostly located in the CCS domain while the DRU is typically found in the Train Control domain. The JRU records data from the ETCS system while the DRU is recording data from other On-Board systems, for instance the TCMS. In the future, other functions than ETCS will reside in the CCS domain (e.g., ATO). Those functions have also a need to record data. Hence, a DRU is proposed to be added to the CCS domain. Whether this is a specific hardware, in addition to the hardware available in the TCMS domain, or the DRU hardware can be combined needs to be explored further.

At least one TRU is installed on every OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the TRU components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.6 Vehicle Locator (VL)

The Vehicle Locator (VL) is a safe CCS On-Board component that uses sensor data and supporting information to provide train location output information safely and reliably. The Vehicle Locator (VL) is able to provide the absolute and relative position in reference to of the front end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles; hence, the VL is more than just an odometry component.

One VL is installed on every OCORA based CCS On-Board system. The sensors connected to it may differ from one installation to the other. Refer to Appendix D1 on page 110 to locate the VL component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.7 Vehicle Locator Sensors (VLSs)

The Vehicle Locator Sensors (VLS) provide raw data to determine speed, direction of travel, acceleration, position, and cold movement information to the Vehicle Locator. Depending on the RU's need and the progress of technology (e.g., GNSS, IMU) different type and quality of sensors may be used.

Multiple Vehicle Locator Sensors are installed on every OCORA based CCS On-Board system, but the configuration of the sensors may differ from one installation to the other. Refer to Appendix D1 on page 110 to locate the V Locator Sensors in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.8 Loop Transmission Module (LTM)

The Loop Transmission Module (LTM) is used for ETCS L1 and L1LS systems to process the data from the Loop Transmission Antenna (LT-Antenna) and makes the data available on the CCN.

The LTM is installed on every OCORA based CCS On-Board system in need Euroloop functionality. Refer to Appendix D1 on page 110 to locate the LTM component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.9 Loop Transmission Antenna (LT-Antenna)

The Loop Transmission Antenna (LT-Antenna) receives data through an RFID interface from the EURO Loop and provides the data to the Loop Transmission Module (LTM).

The LT-Antenna is installed on every OCORA based CCS On-Board system in need of Euroloop functionality. Refer to Appendix D1 on page 110 to locate the LT-Antenna component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.10 Balise Transmission Module (BTM)

The Balise Transmission Module (BTM) is used for ETCS L1 – L3 systems (including L0 and LNTC). It processes the data from the Balise Transmission Antenna (BT-Antenna) and makes the data available on the CCN, for the ETCS application (VS). Optionally, the BTM can also receive data from KER Balises and make the data available, through the CCN, to the corresponding STM using the K interface described in SUBSET-101.

The BTM is installed on every OCORA based CCS On-Board system in need of ETCS functionality. Refer to Appendix D1 on page 110 to locate the BTM component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.11 Balise Transmission Antenna (BT-Antenna)

The Balise Transmission Antenna (BT-Antenna) receives data through an RFID interface from the EURO Balise and provides the data to the Balise Transmission Module (BTM). Optionally, the BT-Antenna can also receive data through an RFID interface from the KER Balises and provide the data to the Balise Transmission Module (BTM).

The BT-Antenna is installed on every OCORA based CCS On-Board system in need of ETCS functionality. Refer to Appendix D1 on page 110 to locate the BT-Antenna component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.12 Specific Transmission Module (STM)

The Specific Transmission Module (STM) represents the peripheral device implementing the STM functionality defined by the STM component of the NTC HW Solution (refer to 4.1.7).

Multiple STMs can be connected to the CCN. They are installed on OCORA based CCS On-Board system on an as needed basis. Refer to Appendix D1 on page 110 to locate the STM components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.13 National Train Control (NTC)

The National Train Control (NTC) represents the peripheral device implementing the NTC functionality defined by the NTC component of the NTC HW Solution (refer to 4.1.7).

Multiple NTCs can be connected via the respective STM to the CCN. They are installed on OCORA based CCS On-Board system on an as needed basis. Refer to Appendix D1 on page 110 to locate the NTC components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.14 National Train Control Antenna (NTC-Antenna)

The National Train Control Antennas (NTC-Antennas) receive the data from the trackside installations of the respective national ATP system and provides the data to the NTC.

The NTC-Antennas can be connected via the respective NTC and STM to the CCN. They are installed on OCORA based CCS On-Board system on an as needed basis. Refer to Appendix D1 on page 110 to locate the NTC-Antenna components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.15 Perception Systems (PSs)

The Perception System (PSs) provides awareness information if needed for GoA3 and GoA4 operations. In case of light signalling perception, the PSs may also be used for GoA1-2 operations. The Perception System processes the data from the various Perception Sensors (P Sensors), performs the necessary sensor fusion, and makes the data available on the CCN.

The PSs are installed on OCORA based CCS On-Board system, if needed for ATO GoA1 – GoA4 operations. Refer to Appendix D1 on page 110 to locate the PSs component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.16 Perception System Sensors (P-Sensors)

The Perception Sensors (P-Sensors) include all sensors to provide enough awareness of the environment (mainly the tracks) for safe GoA3 and GoA4 operations. In case of light signalling perception, the PSs may also be used for GoA1-2 operations. The sensors are mostly cameras, LIDAR and RADAR but can also include vibration sensors, smoke detectors, etc. (refer also to [14], Localisation On-Board – Introduction)

The P-Sensors are installed on OCORA based CCS On-Board system, supporting ATO GoA1 – GoA4. Refer to Appendix D1 on page 110 to locate the P-Sensor components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.2.17 Cab Voice Radio Legacy (CVRL)

The CVRL is used for the communication between the driver and the operations control personnel and in some cases for communication between train staff. Today, it contains a control panel, a microphone, a loudspeaker, and a GSM-R voice radio and may connect directly with the PIS through a legacy connection (e.g., UIC) and to the DMI and/or JRU through respective connections. In current implementations, the CVRL is only loosely integrated into the CCS domain, if at all. But with the upcoming migration from GSM-R to FRMCS options become available to share the new connectivity infrastructure, the FRMCS On-Board System (5.3.1), between the CCS data and cabin voice.

The OCORA concept foresees providing voice communication services through the FRMCS On-Board System and to connect the CVRL to the PIS, DMI and the JRU the through the CCN. To allow the CVRL using these new services, the CVRL needs to be adapted to connect to the CCN and to use the services provided by the FRMCS On-Board System and the OCORA CCS On-Board.

The CVRL is an optional deployment on OCORA based CCS On-Board system. Refer to Appendix D1 on page 110 to locate the CVRL peripheral device in the OCORA architecture. In situations, where the train is running on FRMCS based infrastructure only, the need of a dedicated CVRL vanishes and the communication between the driver, the operations control personnel and the train staff can be provided by using the OCORA based solution consisting of the CVD (refer to 5.2.2), the CVR Application (4.15) running on the OCORA platform and the FRMCS On-Board System (5.3.1) providing the connectivity.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.3 Connectivity devices

The connectivity devices are components outside the "OCORA Core" scope. For these components, OCORA only provides interface specifications, high-level functional requirements, and non-functional requirements. Basically, all requirements and specifications needed to ensure "plug & play"-like exchangeability. Of course, these specifications are only developed for the building blocks not already standardised (well enough) or where no standard is being developed by other organizations. The connectivity devices are also considered for all RAMSS aspects.

The connectivity devices provide secure connectivity to the data centres for the CCS On-Board domain. Eventually, other domains such as the train control or the passenger information may use this infrastructure for their communication needs. Refer to Appendix B for a discussion of possible options.

There are several possible scenarios for the network topology and how to segment the different On-Board network(s). Appendix A provides a detailed explanation and a view in relation to train integration. Cyber security aspects for the different scenarios and a discussion for the further evaluation of the preferable scenario are detailed in Appendix B and B5.

Summary of the scenarios:

#	Title	Description
A	**Scenario A:** **CCN as physically separated network**	The CCS and the TCMS are running on physically separated Ethernet Consist Networks (ECN) and are interconnected through a gateway (ECN/ECN Security Gateway) providing routing and cyber security functionality between the two networks (CCN and NG-TCN). The FRMCS On-Board System and any other connectivity system (e.g., MCG) are located on a separate connectivity network providing trackside connectivity and to address cyber security requirements.
B	**Scenario B:** **CCN as logically separated network**	The control systems, CCS and TCMS, are using the same physical network with logical segmentation between the CCN and NG-TCN. Non-control systems like Passenger Information System are attached to a physically segmented network – the Operator Network. The FRMCS On-Board System and any other connectivity system (e.g., MCG) are located on a separate connectivity network providing trackside connectivity and to address cyber security requirements.
C	**Scenario C:** **Common critical control network logically separated**	The control systems, CCS and TCMS, are using the same physical network. The CCS and the critical control components of the TCMS are logically separated from the no-critical control components of the TCMS. Non-control systems like Passenger Information System are attached to a physically segmented network – the Operator Network. The FRMCS On-Board System and any other connectivity system (e.g., MCG) are located on a separate connectivity network providing trackside connectivity and to address cyber security requirements.
D	**Scenario D:** **Common critical control network physically separated**	The critical control systems, CCS and critical TCMS components are using the same physical network. Non-critical control components of the TCMS, non-control systems like Passenger Information System are attached each to its own physically segmented network. The FRMCS On-Board System and any other connectivity system (e.g., MCG) are located on a separate connectivity network providing trackside connectivity and to address cyber security requirements.
E	**Network architecture for retrofit vehicles**	The CCS is running on the OCORA CCN and is connected to a legacy vehicle using the OCORA-GW for physical and logical adaptation. The FRMCS On-Board System and any other connectivity system (e.g., MCG) are located on a separate connectivity network providing trackside connectivity and to address cyber security requirements. **Remark:** This scenario will cannot be evaluated against the ones having a NG-TCN, since it is related to the integration into an existing train with a legacy network technology.

Table 20 Possible scenarios for the network topology and train integration

5.3.1 FRMCS On-Board System

The FRMCS On-Board System implements the required functionalities and services providing the connectivity for the CCS Systems with the RBC (for ETCS L2/L3 networks), with ATO trackside (ATO-AT) and with the RCA compliant CCS Data Centres respectively.

The FMRCS On-Board System runs on a dedicated hardware platform in a separate communication network to allow its services to be shared with other, non-CCS applications. This assures, that cybersecurity aspects are covered, and appropriate zoning models can be applied to the On-Board communication networks.

The FRMCS On-Board System is currently being specified by the TOBA working group and will interface with several On-Board applications as specified in the FRMCS User Requirements Specification [44].

5.3.2 FRMCS Radio

The FRMCS Radio represents a modem with one or more 3GPP and/or non-3GPP radio access technologies supported by the FRMCS system.

Multiple FRMCS Radio modules may be installed on every OCORA based CCS On-Board system supporting cabin voice and/or ETCS L2 or higher level as well as other On-Board Applications, once FRMCS is available. Refer to Appendix D1 on page 110 to locate the FRMCS Radio components in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.3.3 GSM-R - EDOR Radio

The GSM-R EDOR Radio provides (cyber-)secure GSM-R data connectivity to trackside systems. Today, it is mainly used for the communication with the RBC in case of ETCS level 2 operations. The device will become obsolete when FRMCS is rolled out on all trackside infrastructures.

The GSM-R EDOR Radio is installed on every OCORA based CCS On-Board system supporting ETCS L2 or higher, if FRMCS is not widely deployed. Refer to Appendix D1 on page 110 to locate the GSM-R EDOR Radio component in the OCORA architecture.

Depending on the vehicle and retrofit scenario, the GSM-R radio modems may be connected directly to a CCU running the ETCS application to avoid unnecessary changes on the existing CCS equipment or applications.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.3.4 Mobile Communication Gateway CCS (MCG CCS)

The Mobile Communication Gateway (MCG CCS) provides train to track-side connectivity for the On-Board CCS in case the trackside service is not available through FRMCS. Depending on the vehicle, it may also provide track-side connectivity for the systems (e.g., TCMS and PIS) of the Train Communication Networks.

For communication over public radio networks (remote diagnostics and maintenance), a corresponding modem might be integrated or connected to the MCG CCS.

The MCG CCS is connected to a separate communication network to protect the On-Board networks from potential cyber security attacks originating from trackside.

5.3.5 Public Radio

The Public Radio provides connectivity between the train and off-board. The OCORA architecture foresees that multiple Public Radio modems can be connected to the MCG CCS, depending on the RU's need. Public Radio connections are mainly used for monitoring, diagnostic, and maintenance purposes during the transition phase to FRMCS. Separate modems can connect the train with the operations centre of its RU and/or with the train supplier. The Public Radio modem will eventually be replaced by the respective functionality of the FRMCS Radio.

Multiple Public Radios can be installed on OCORA based CCS On-Board system on an as needed basis. Refer to Appendix D1 on page 110 to locate the Public Radio component in the OCORA architecture.

Further details will be provided in subsequent versions of the OCORA architecture documentation.

5.3.6 Com Network

The Communication Network is a standard IP network over Ethernet IEEE 802.3 where the communication systems (FRMCS On-Board System and MCG) for the trackside connectivity are attached. This separation from the other On-Board networks allows to apply appropriate zoning models addressing cybersecurity requirements.

5.3.7 Sec Network

The Security Network is a standard IP network over Ethernet IEEE 802.3 where the security systems for the On-Board Security Services (OSS) are attached. This separation from the other On-Board networks allows to apply appropriate zoning models addressing cybersecurity requirements.

5.3.8 Aux Network

The Auxiliary Network is a standard IP network over Ethernet IEEE 802.3 where the non-critical control components of the TCMS domain, the auxiliary components (e.g., toilets, climate and lighting) are located.

5.3.9 On-Board Security Services – OSS

The On-Board Security Services encompasses the applications and services to assure cyber secure operations of the On-Board systems and networks.

Although the OSS are not in the scope of OCORA, the architecture and network topology discussion do consider the OSS and its required components in regards of the allocation and integration of these services.

Services considered as such OSS:

- System-wide time service
- Central logging
- Identity and Access Management
- Backup
- Asset inventory
- Intrusion detection / continuous security monitoring
- Public Key Infrastructure
- Domain Name Service

5.3.10 Public Wi-Wi

The Public Wi-Fi providing public Wi-Fi to the passengers of the train is not in the scope of the OCORA reference architecture. It is shown on the physical architecture to indicate the independence from any CCS On-Board system and network.

6 External interfaces of CCS On-Board (CCS-OB)

This chapter identifies and describes all external interfaces for the CCS On-Board (CCS-OB). The content in this chapter represents the current state of work. The chapter will evolve with the OCORA collaboration.

6.1 Mechanical interfaces

Information will be provided in subsequent versions of this document.

6.2 Electrical interfaces

Information will be provided in subsequent versions of this document.

6.3 Communication interfaces (OSI layers 1-6)

The following pictures identify all external communication interface for OSI layers 1-6 for CCS On-Board (CCS-OB). The table following the graphics provides a high-level description for every interface.

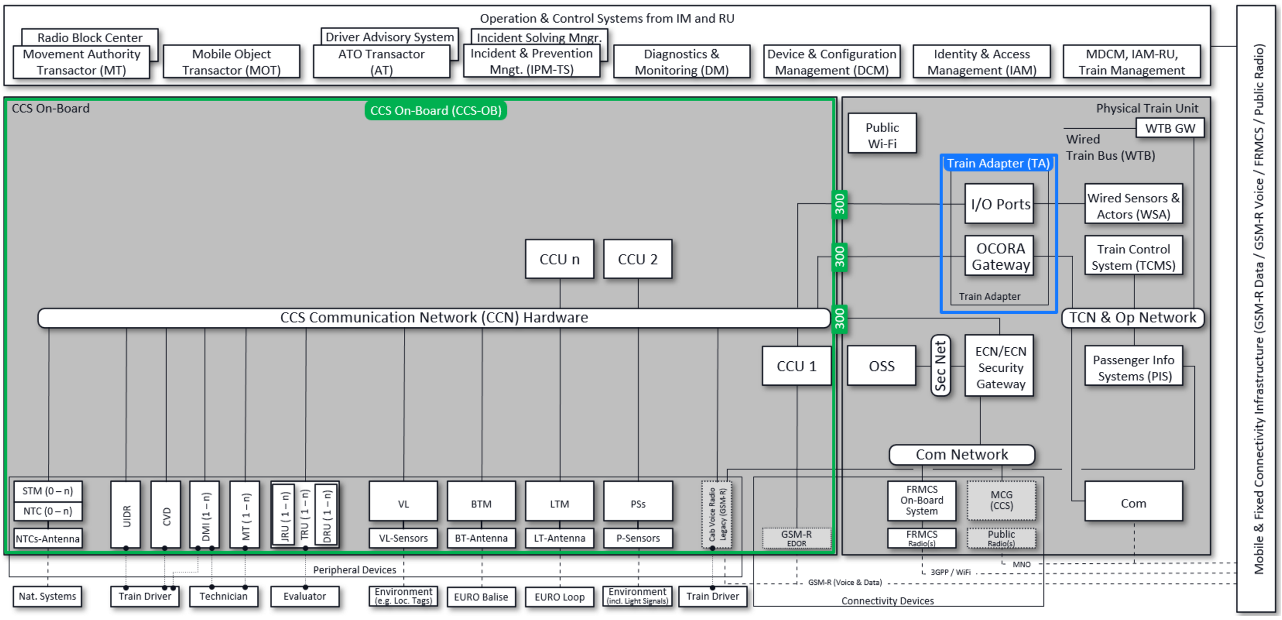

Figure 15 CCS-OB physical architecture with external communication IFs (OSI layers 1-6)

(refer to Appendix D1 on page 110 for large scale representation)

Interface ID	High-Level Description
300	This is the interface, the CCS Communication Network (refer to chapter 5.1.1) provides to the I/O Ports (refer to chapter 2.2.4.2), the OCORA Gateway (refer to chapter 2.2.4.2), and possibly to the connectivity devices connected through the ECN/ENC Security Gateway (refer to chapter 2.4.3). The interface is currently defined for OSI layer 1 to 2 (refer to OCORA OSI definitions in document [10]) but will be specified up to OSI layer 6 and 7 (refer to OCORA OSI definitions in document [10]) in subsequent versions of the OCORA specifications.

Table 21 External communication IFs of the “CCS On-Board” scope (OSI layers 1-6)

6.4 Communication interfaces (OSI layer 7)

The following pictures identify all external communication interface on OSI layer 7 for the CCS On-Board (CCS-OB). The table following the graphics provides a high-level description for every interface.

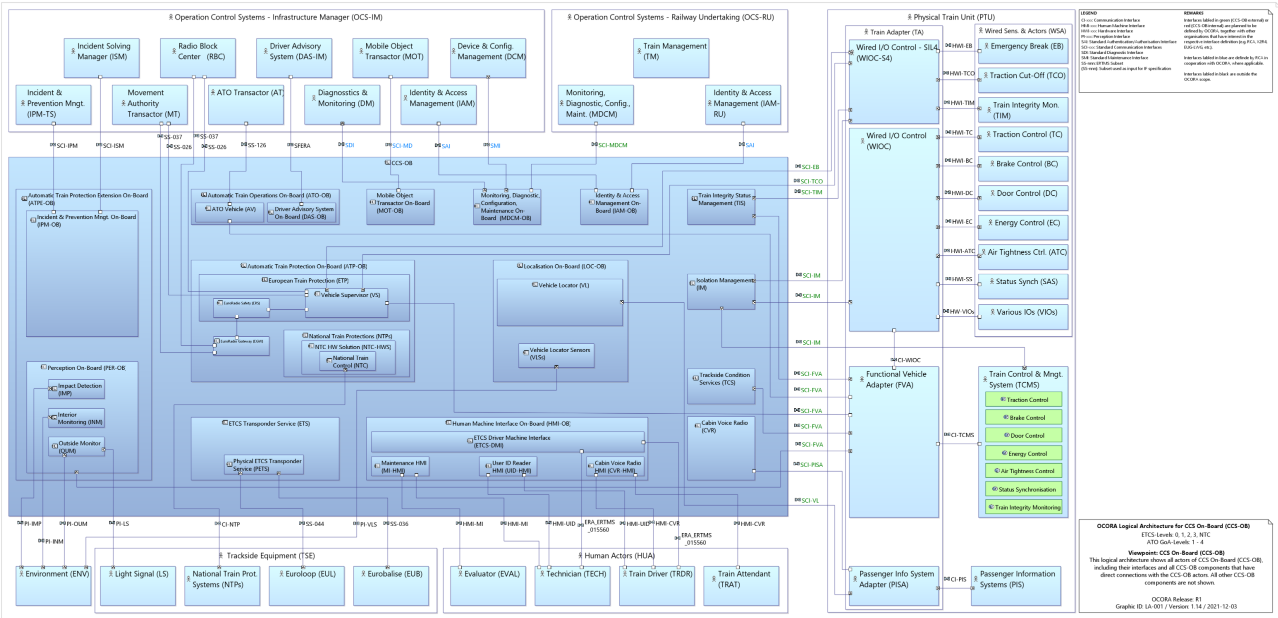

Figure 16 CCS-OB logical architecture with external communication IFs (OSI layer 7)

(refer to Appendix D3 on page 112 for large scale representation)

Interface ID	High-Level Description
SCI-ISM	**Standard Communication Interface – Incident Solving Manager** This is the standard communication interface of the Incident Solving Manager (ISM) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-IPM	**Standard Communication Interface – Incident & Prevention Management** This is the standard communication interface of the Incident & Prevention Management (IPM-TS) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SS-026	This is the interface between the Vehicle Supervisor (refer to chapter 4.1.2) and the Advanced Protection System's Movement Authority Transactor (MT) or the Radio Block Center (RBC), depending on the system provided by the infrastructure manager. SUBSET-026, chapter 7 & 8 define this interface.
SS-037-SaSAP	**SUBSET-037 - Safety Service Access Point** This is the interface between the safety service user (e.g., ATP-OB application) and the Safe Functional Module (SFM) of the EuroRadio Protocol. Refer also to Chapter 4.1.3 for further information.
SS-037-TSAP	**SUBSET-037 - Transport Service Access Point** This is the interface between the Safe Functional Module (SFM) and the Communication Functional Module (CFM) of the EuroRadio Protocol. Refer also to Chapter 4.1.3 for further information.

Interface ID	High-Level Description
SS-126	This is the interface between the ATO Vehicle (4.4.1) and the ATO Transactor (AT). SUBSET-126 is being prepared by S2R to specify this interface.
SFERA	This is the interface between Driver Advisory System On-Board (4.4.2) and the Driver Advisory System (DAS-IM) of the infrastructure manager. SFERA aims at providing a standard for this interface.
SCI-MD	**Standard Communication Interface – Mobile Object Transactor** This is the interface between the Mobile Object Transactor On-Board (4.6) the Advanced Protection System's Mobile Object Transactor (MOT). This interface is used by the Mobile Object Transactor On-Board to send localisation data to the MOT, containing e.g., ETCS irrelevant data (not used by VS). This interface is being standardized by RCA.
SDI	This is the interface between On-Board Monitoring, Diagnostic. Configuration, Maintenance component (refer to chapter 4.7) and the Diagnostic & Monitoring system (DM) of the infrastructure manager, the vehicle currently operates in. This interface is defined by RCA. Refer to document [30].
SMI	This is the interface between On-Board Monitoring, Diagnostic. Configuration, Maintenance component (refer to chapter 4.7) and the Device & Configuration Management system (DCM) of the infrastructure manager, the vehicle currently operates in. This interface is defined by RCA. Refer to document [30].
SCI-MDCM	**Standard Communication Interface – Monitoring, Diagnostic, Configuration, Maintenance** This is the interface between On-Board Monitoring, Diagnostic, Configuration, Maintenance component (refer to chapter 4.7) and the Device & Configuration Management system (MDCM) of the railway undertaking. OCORA aims at providing a standard for this interface.
SAI	This is the interface between Vehicle Identity & Access Management (refer to chapter 2.3.8) and the Identity & Access Management system (IAM) of the infrastructure manager, the vehicle currently operates in, and/or the Identity & Access Management system (IAM-RU) of the railway undertaking. This interface is defined by RCA. Refer to document [30].
SCI-EB	**Standard Communication Interface – Emergency Brake** This is the standard communication interface between the Vehicle Supervisor (4.1.2) and the Wired I/O Control – SIL4 actor (WIOC-S4) to control the Emergency Brake device of the Physical Train Unit (PTU). OCORA aims at providing a standard for this interface.
SCI-TCO	**Standard Communication Interface – Traction Cut-Off** This is the standard communication interface between the Vehicle Supervisor (4.1.2) and the Wired I/O Control actor (WIOC) to control the Traction Cut-Off device of the Physical Train Unit (PTU). OCORA aims at providing a standard for this interface.
SCI-TIM	**Standard Communication Interface – Train Integrity Status Management** This is the standard communication interface between the Wired I/O Control – SIL4 actor (WIOC-S4) of the Physical Train Unit and the Train Integrity Status Management component (4.12) to monitor the integrity of the Physical Train Unit (PTU). OCORA aims at providing a standard for this interface.
SCI-IM	**Standard Communication Interface – Isolation Management** This is the standard communication interface between the Isolation Management component (4.13) and the actors of the Physical Train Unit, requiring the isolation status of the CCS On-Board. Consumers of this interface are the Wired I/O Control – SIL4 actor (WIOC-S4), the Wired I/O Control actor (WIOC) and the Train Control & Management System (TCMS) of the Physical Train Unit. OCORA aims at providing a standard for this interface.

Interface ID	High-Level Description
SCI-FVA	**Standard Communication Interface – Functional Vehicle Adapter** This is the standard communication interface between the CCS On-Board and the Functional Vehicle Adapter (FVA) of the Physical Train Unit. OCORA aims at providing a standard for this interface.
SCI-VL	**Standard Communication Interface – Vehicle Locator** This is the standard communication interface between the Vehicle Locator (4.3.1) and Passenger Info System Adapter (PISA) of the Physical Train Unit providing location information to be used by the Passenger Information System (PIS). OCORA aims at providing a standard for this interface.
SCI-PISA	**Standard Communication Interface – Passenger Info System Adapter** This is the standard communication interface between the Cab Voice Radio (4.15) and the Passenger Info System Adapter (PISA) on trains equipped with a NG-TCN. OCORA aims at providing a standard for this interface.
HMI-CVR	This is the interface between the Cabin Voice Radio HMI (refer to chapter 4.16.4) and the Train Driver (TRDR). OCORA does not aim to standardize this interface.
ERA_ERTMS_015560	This is the interface between the Driver Machine Interface (refer to chapter 5.2.3) and the Train Driver (TRDR) or the Technician (TECH). Standardization efforts for ETCS functionality are ongoing by the ERA (refer to document [41] , ERA_ERTMS_015560). The document must be extended to include ATO requirements (not in scope of OCORA). Standardization of the user interfaces for Voice Radio, Diagnostics, Monitoring, Configuration, NTCs, and Driver Advisory Vehicle are not existing and OCORA does not plan, at this point in time, to work on those standards.
HMI-UID	This is the interface between the User Identification Reader (refer to chapter 5.2.1) and the Train Driver (TRDR) or the Driver's UID card. OCORA does not aim to standardize this interface.
HMI-MI	This is the interface between the Maintenance Terminals (refer to chapter 5.2.4) and the Technician (TECH) or the Evaluator (EVAL). OCORA does not aim to standardize this interface.
PI-VLS	These is are the interface between the Vehicle Locator Sensors (refer to chapter 5.2.7) and their environment (ENV) that can include a trackside mounted Location Tag. OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
SS-044	This is the interface between the Physical ETCS Transponder Service (The PETS component reads the ETCS telegrams from the trackside installed infrastructure (Eurobalise and Euroloop) and forwards them to the CCS On-Board applications.) and the Euroloop (EUL) using the Loop Transmission Antenna (refer to chapter 5.2.9). SUBSET-044 specifies this interface.
SS-036	This is the interface between the Physical ETCS Transponder Service (The PETS component reads the ETCS telegrams from the trackside installed infrastructure (Eurobalise and Euroloop) and forwards them to the CCS On-Board applications.) and the Eurobalise (EUB) using the Balise Transmission Antenna (refer to chapter 5.2.11). SUBSET-036 specifies this interface.
CI-NTP	This is the interface between the trackside National Train Protection systems (NTPs) and the On-Board National Train Control system (refer to chapter 5.2.13). This is a specific interface of the existing National ATP systems and is therefore not relevant for OCORA.

Interface ID	High-Level Description
PI-IMP	This is the interface between the sensors of the Impact Detection component (refer to chapter 4.2.3) and their environment (ENV). OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
PI-INM	This is the interface between the sensors of the Interior Monitor component (refer to chapter 4.2.4) and their environment (ENV). OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
PI-OUM	This is the interface between the sensors of the Outside Monitor component (refer to chapter 4.2.5) and their environment (ENV). OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
PI-LS	This is the interface between the sensors of the Outside Monitor component (refer to chapter 4.2.5) and their environment (ENV). OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.

Table 22 External communication IFs of the “CCS On-Board” scope (OSI layers 7)

7 Internal interfaces of the CCS On-Board (CCS-OB)

This chapter identifies and describes all interfaces for the CCS On-Board (CCS-OB). The content in this chapter represents the current state of work. The chapter will evolve with the OCORA collaboration.

7.1 Mechanical interfaces

Information will be provided in subsequent versions of this document.

7.2 Electrical interfaces

Information will be provided in subsequent versions of this document.

7.3 Communication interfaces (OSI layers 1-6)

The following picture identifies all internal communication interface for OSI layers 1-6 for CCS On-Board (CCS-OB). The table following the graphic provides a high-level description for every interface.

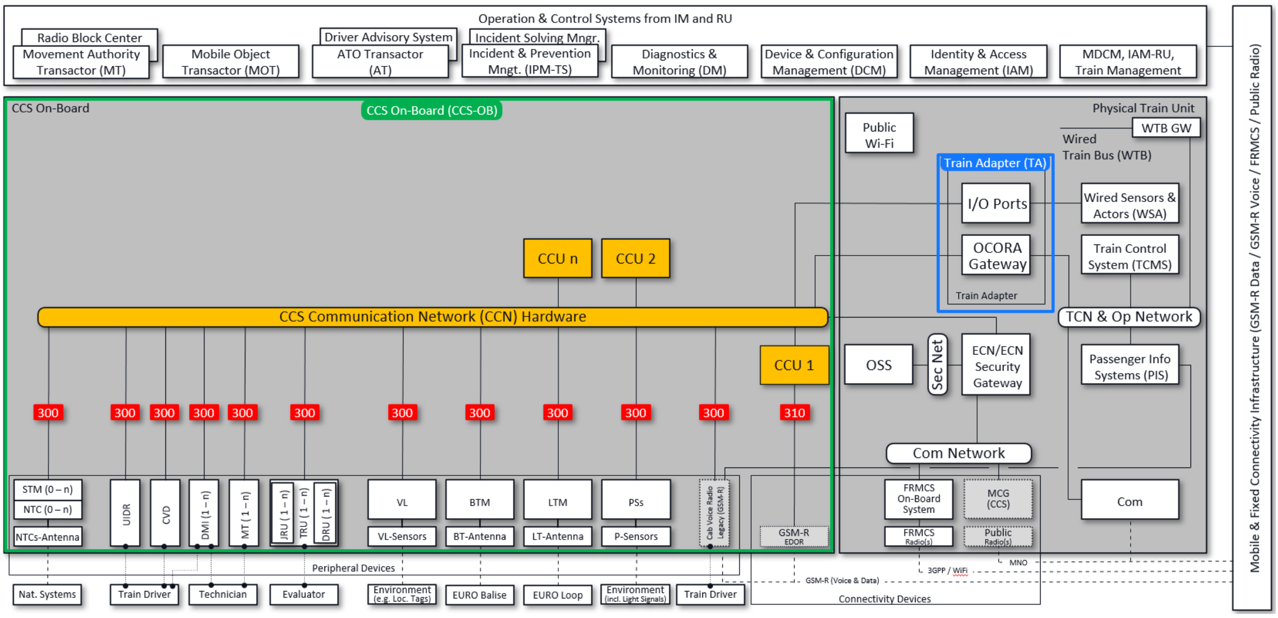

Figure 17 CCS-OB physical architecture with internal communication IFs (OSI layers 1-6)

(refer to Appendix D2 on page 111 for large scale representation)

Interface ID	High-Level Description
300	This is the interface, the CCS Communication Network (refer to chapter 5.1.1) provides to the CCUs (refer to chapter 5.1.2), the OCORA Gateway (refer to chapter 2.2.4.2), all the peripheral devices (refer to chapter 5.2). The interface is currently defined for OSI layer 1 to 2 (refer to OCORA OSI definitions in document [10]) but will be specified up to OSI layer 6 and 7 (refer to OCORA OSI definitions in document [10]) in subsequent versions of the OCORA specifications.
310	This interface is required during a migration phase, where FRMCS is not completely rolled out on the infrastructure side. It connects the GSM-R ETCS Data Only Radio to the CCU running the ETCS respectively the ATP On-Board application.

Table 23 Internal communication IFs of the “CCS On-Board” scope (OSI layers 1-6)

7.4 Functional interfaces (OSI layer 7)

The following picture identifies all internal communication interfaces on OSI layer 7 for the CCS On-Board (CCS-OB). The table following the graphic provides a high-level description for every interface.

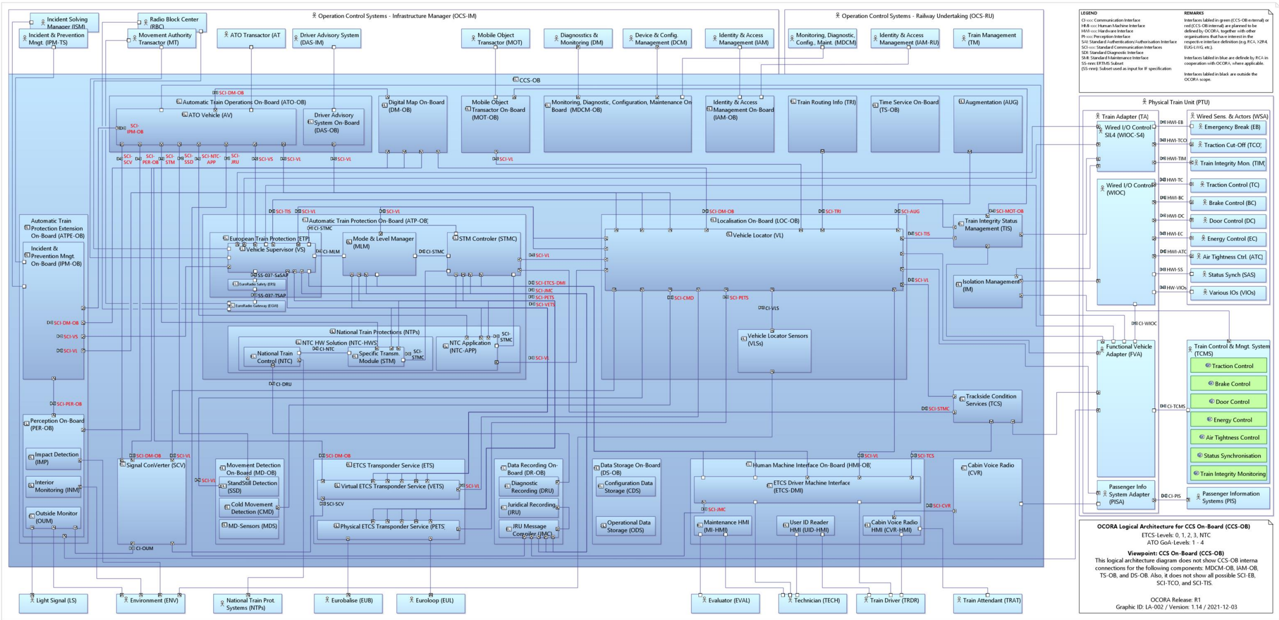

Figure 18 CCS-OB logical architecture with internal communication IFs (OSI layer 7)

(refer to Appendix D4 on page 113 for large scale representation)

Interface ID	High-Level Description
SCI-AUG	**Standard Communication Interface – Augmentation** This is the standard communication interface of the Augmentation component (4.11) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-CMD	**Standard Communication Interface – Cold Movement Detection** This is the standard communication interface of the Cold Movement Detection component (4.20.2) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-CVR	**Standard Communication Interface – Cabin Voice Radio** This is the standard communication interface of the Cabin Voice Radio component (4.15) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-DM-OB	**Standard Communication Interface – Digital Map On-Board** This is the standard communication interface of the Digital Map On-Board component (4.5) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-ETCS-DMI	**Standard Communication Interface – ETCS DMI** This is the standard communication interface of the ETCS DMI component (4.16.1) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-IPM-OB	**Standard Communication Interface – Incident & Prevention Management On-Board** This is the standard communication interface of the Incident & Prevention Management On-Board component (4.2.1) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.

Interface ID	High-Level Description
SCI-JMC	**Standard Communication Interface – JRU Message Compiler** This is the standard communication interface of the JRU Message Compiler (4.18.3). SUBSET-027 defines the data stored in the JRU and SUBSET-140 is being prepared for ATO data storage. However, the DRU data is not standardized and the access to the JRU and DRU is not standardized. OCORA may consider standardizing the JRU output format to facilitate data evaluation with a vendor independent evaluation software and integration into standardised remote monitoring. OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-JRU	**Standard Communication Interface - JRU** This is the standard communication interface of the JRU (4.18.2) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-MOT-OB	**Standard Communication Interface – Mobile Object Transactor On-Board** This is the standard communication interface of the Mobile Object Transactor On-Board component (4.6) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-NTC-APP	**Standard Communication Interface – National Train Control Application** This is the standard communication interface of the National Train Control Application (4.1.10) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-PER-OB	**Standard Communication Interface – Perception On-Board** This is the standard communication interface of the Perception On-Board component (4.2.2) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-PETS	**Standard Communication Interface – Physical ETCS Transponder Service** This is the standard communication interface of the Physical ETCS Transponder Service (4.19.2) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-SCV	**Standard Communication Interface – Signal Converter** This is the standard communication interface of the Signal Converter component (4.21) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-SSD	**Standard Communication Interface – Stand Still Detection** This is the standard communication interface of the Stand Still Detection component (4.20.1) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-STM	**Standard Communication Interface – Specific Transmission Module** This is the standard communication interface of the Specific Transmission Module component (4.1.9) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-STMC	**Standard Communication Interface – STM Controller** This is the standard communication interface of the STM Controller component (4.1.5) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-TCS	**Standard Communication Interface – Trackside Condition Service** This is the standard communication interface of the Trackside Condition Service (4.14) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.

Interface ID	High-Level Description
SCI-TIS	**Standard Communication Interface – Train Integrity Status** This is the standard communication interface of the Train Integrity Status component (4.12) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-TRI	**Standard Communication Interface – Train Routing Info** This is the standard communication interface of the Train Routing Info component (4.9) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-VETS	**Standard Communication Interface – Virtual ETCS Transponder Service** This is the standard communication interface of the Virtual ETCS Transponder Service (4.19.1) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-VL	**Standard Communication Interface – Vehicle Locator** This is the standard communication interface of the Vehicle Locator (4.3.1) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.
SCI-VS	**Standard Communication Interface – Vehicle Supervisor** This is the standard communication interface of the Vehicle Supervisor (4.1.2) OCORA aims at standardizing this interface. Details will be provided in subsequent versions of the OCORA Architecture.

Table 24 Internal logical IFs of the “CCS On-Board” scope (OSI Layer 7)

8 Train Unit (TU) internal interfaces

The following Table provides an overview and a brief description of the PTU internal interfaces which are of interest for the CCS On-Board but not in the scope of the CCS On-Board

Interface ID	High-Level Description
HWI-EB	Hardware Interface between the Wired I/O Control SIL4 component (WIOC-S4) and the wired Emergency Brake actor.
HWI-TCO	Hardware Interface between the Wired I/O Control SIL4 component (WIOC-S4) and the wired Traction Cut-Off actor.
HWI-TIM	Hardware Interface between the Wired I/O Control SIL4 component (WIOC-S4) and the wired Train Integrity Monitoring sensor(s).
HWI-TC	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Traction Control actor. .
HWI-BC	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Brake Control actor.
HWI-DC	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Door Control actor.
HWI-EC	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Energy Control actor.
HWI-ATC	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Air Tightness Control actor.
HWI-SS	Hardware Interface between the Wired I/O Control component (WIOC) and the wired Status Sync actor/sensor.
HWI-VIOs	Hardware Interface between the Wired I/O Control component (WIOC) and various I/O actors/sensors.
CI-WIOC	Communication interface between the Functional Vehicle Adapter (FVA) and the Wired I/O Controls of the Train Adapter (TA)
CI-TCMS	Communication interface between the Functional Vehicle Adapter (FVA) and the Train Control & Management System (TCMS)
CI-PIS	Communication interface between the Passenger Information System Adapter (PISA) and the Passenger Information Systems (PIS)

Table 25 Train Unit Internal IFs not in “CCS On-Board” scope

These are existing discrete interfaces on the Physical Train Unit. OCORA does not aim to standardize these interfaces.

9 Computing platform

9.1 Context

The computing platform provides the infrastructure required for operating OCORA's modular, software-component-based, distributed functional CCS On-Board applications. Safety and non-safety critical applications shall be able to coexist on the same platform and may even run on the same computing hardware.

9.2 Motivation

The incentive to postulate an open, standardised computing platform is directly derived from the OCORA problem statements, key principles, objectives, and design statements as described in [7] and [9].

Todays deployed CCS On-Board systems are proprietary, monolithic vendor specific solutions, creating undesired vendor lock-ins resulting in very high cost of ownership. High-priced changes and extensions stall advancements and impede new game-changing technologies.

Safety functions implemented by CCS On-Board systems demand adherence to railway specific standards during development, operation, and maintenance of the entire systems. The stringent homologation processes imposed by CENELEC (standards such as EN50126, EN50128, EN50129) is exorbitantly expensive and time consuming when applied to proprietary, monolithic products in every (type of) rolling stock.

OCORA aims to mitigate the problem by breaking down the CCS On-Board system into different layers and components with defined, open interfaces that can be developed, tested, and certified independently.

The proposed computing platform provides a communication focused abstraction layer; a construction kit for building functional applications, agnostic of the underlying operating system, board support package, hypervisor, and hardware.

Today's monolithic solutions block innovative new application development due to

- lacking support for new functions, sensors, and actuators
- lacking ability to cope with increased/different processing requirements (like real-time/non-real time)
- lacking support for calculation intense machine learning algorithms that require GPU hardware processing.

The OCORA computing platform pursues to address these issues by abstracting the underlying hardware, board support package and operating system. An open, unified platform independent API shall open the door to platform agnostic application development while entrusting the computing platform internals to experienced vendors.

Industrial and technological readiness are essential, when deploying new CCS components. To meet this target, a computing platform that is deployed on a large scale must have been extensively field tested (e.g., to ensure reliability in operation). It will take several computing platform iterations to achieve all OCORA goals (e.g., full hardware independency may not be achieved in the first computing platform generation). Along the journey, applications' portability will be indispensable to leverage implementation and certification effort across the evolving computing platform generations.

9.3 High-level computing platform architecture

The notion of a Platform Independent API is key to the proposed computing platform architecture. It allows vendors to offer solutions readily available on the market as well as new solutions currently in their product pipelines. New and innovative approaches to Safety and Fault Tolerance may be introduced as they become available on the market, promoting a solution agnostic and future-proof evolution of the computing platform whilst functional applications implementing the business logic of CCS On-Board functions remain portable.

A second abstraction considers the different life-cycle profiles of software and hardware. A CCS On-Board system comprises of different hardware modules: on one hand the computing nodes that run the CCS On-Board functional applications and on the other hand all peripheral devices and the external systems (accessed via the ECN/ECN Security Gateway, the OCORA Gateway and I/O Ports).

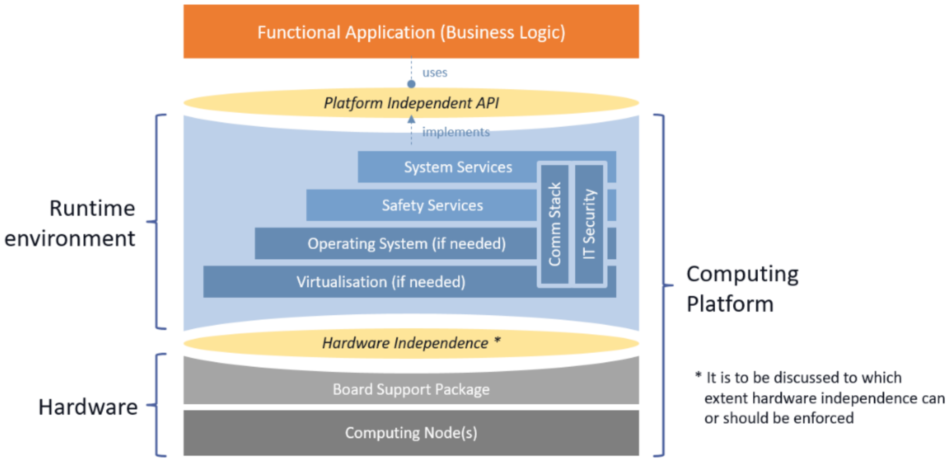

Figure 19 Generalised abstractions – the key to independence

9.3.1 Platform Independence

In OCORA's distributed component based eco-system, a Platform Independent API provides the software layer that lies between the computing platform and the functional applications. It enables the various OCORA components to communicate and share data. Taking advantage of the CCS Communication Network (CCN), the API simplifies the development of such a distributed system by letting software developers focus on the specific purpose of their applications rather than the mechanics of passing information between applications, peripheral devices, and external systems (via the ECN/ECN Security Gateway, the OCORA Gateway and I/O Ports).

The Platform Independent API abstracts the application from the details of the operating system, network transport, and low-level data formats. The same concepts and APIs may be accessible from different programming languages allowing applications to exchange information across operating systems, languages, and processor architectures. Low-level details like data wire format, discovery, connections, reliability, protocols, QoS management, etc. are all managed by the computing platform.

In a component-based architecture communication is the "glue" holding everything together and as such becomes a crucial part of the solution: failing inter-component communication may result in complete system failure.

Safety critical (SIL-4) CCS functional applications must comply with the safety requirements according to CENELEC EN 50126, EN 50128, EN 50129 and EN 50159. In conclusion, the computing platform must comply with the same standards, providing a fully transparent safety and fault tolerance layer.

Applications implemented against the Platform Independent API shall be portable between different computing platform implementations and/or versions. To be able to achieve portability, functional applications may only contain business logic related safety code (like for example the computation of the braking curves), all other safety and fault tolerance aspects are to be handled transparently within the computing platform.

9.3.2 Hardware independence

Hardware independence is key to overcome monolithic vendor specific solutions that create undesired vendor lock-ins. OCORA's computing platform addresses hardware independence on two levels:

Level 1: The introduction of the CCS Communication Network (CCN) provides standardised access to peripheral devices and external systems (via the ECN/ECN Security Gateway, the OCORA Gateway and I/O Ports). Communication is handled by dedicated platform communication services accessible to applications via the Unified Platform Independent API.

Level 2: The computing platform comprises a software part (Run-time Environment) and a hardware part consisting of one ore multiple computing nodes. Computing-node hardware independence is strongly related to the proposed industry solution. In case outright level 2 hardware independence cannot be achieved, potential platform suppliers may be contractually obliged to support and maintain computing-node hardware modules of at least two independent hardware manufactures during the entire lifetime of the computing platform.

9.4 Design paradigms and platform approaches

The computing platform architecture shall follow the below design paradigms:

- **Clear separation of concern between the functional applications and the platform:** Notably, functional applications shall handle only business logic, while all other required functions to maintain the application's life-cycle (incl. mechanisms for safety, fault tolerance, persistence, communication, and application management) shall be handled by the computing platform;
- **Satisfy railway norms such as EN 50126, EN 50128 and EN 50129 in their application for up to SIL4:** provide functional applications with the safe, reliable, deterministic, and real-time performance as well as the level of availability required.
- **Provide a mechanism for Safe and Secure Communication with external entities:** (peripheral devices and external systems via the ECN/ECN Security Gateway, the OCORA Gateway and I/O Ports)
- **Provide mechanisms to sufficiently isolate functional applications:** in particular when involving different SIL levels, that are running on the same physical platform.
- **Implement a harmonized Platform Independent API:** possibly common between On-Board and track-side implementations
- **Follow a modular safety concept:** to minimize homologation efforts
- **Maximize usage of COTS hardware components:** to be able to choose the hardware according to the required performance, availability, processor architecture, etc. and to minimize vendor lock-in and leverage advances in other sectors.
- **Consider utilizing virtualization techniques or similar means of abstraction of compute resources:** for better evolvability, scalability, the support of mixed SIL constellations and a more flexible mapping of applications to compute resources.

The computing platform's exact internal architecture is intentionally entrusted to the industry e.g., potential platform vendors. Depending on existing solutions, but whilst respecting above mentioned design paradigms, vendors may propose completely different approaches.

The below diagram depicts four possible options on how the internals of the computing platform could look like. The presented options are intended to illustrate the idea only.

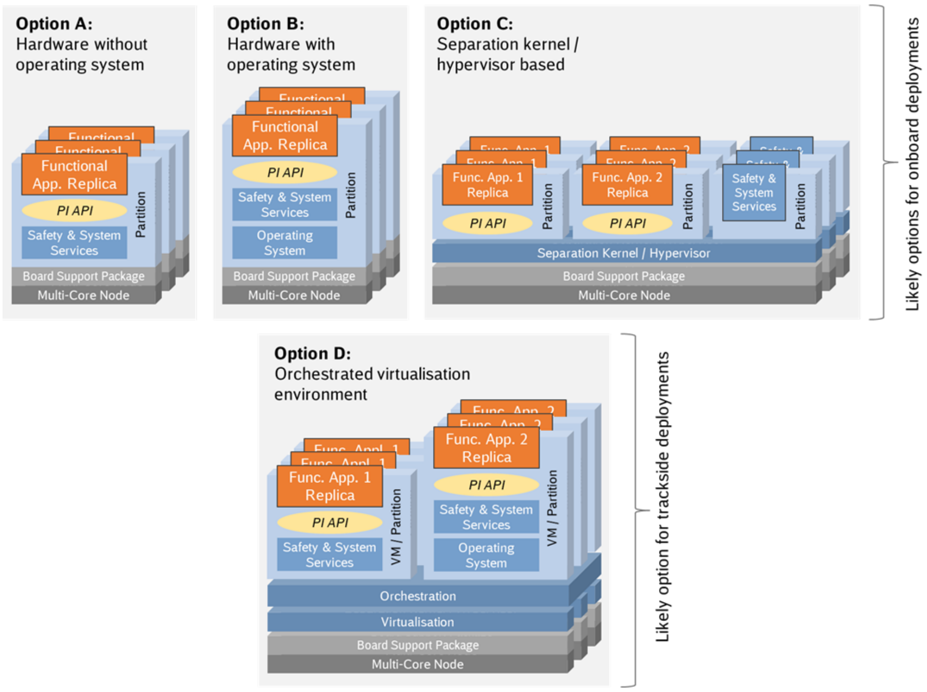

Figure 20 Platform approaches

The *Functional Application* is a functional module of the over-all-system. It has its own task (business logic). It interfaces with the computing platform via a unified platform independent API and runs in a *Partition*.

Partitions are execution environments with guaranteed memory address space isolation and limited processor (or core) execution time. Propagation of software errors among partitions is assured to be impossible. To be consistent, the concept of a *Partition* is also applied to systems without virtualisation. They comply by default with afore mentioned partition characteristics.

The functional application does not depend on how the underlying system is built and which mechanism is used to achieve the required safety, availability, and performance. For instance, a supplier could in principle realise the platform based on embedded hardware, e.g., on “bare metal” or with an operating system, as depicted as **options A and B** in Figure 13, respectively. In such case, if a composite fail safety approach is used, each functional application replica of each application would run on a dedicated multi-core node.

A more future-proof solution allowing to integrate multiple functional applications over a common set of computing nodes would be to involve a separation kernel and / or hypervisor, in the figure shown as **option C**. In this case, multiple functional applications could coexist on the same multi-core node, though the functional application replica belonging to the same application would have to run on separate notes.

While the three mentioned options could be suitable for onboard deployments, it is expected that larger scale trackside data centres would rather be based on orchestrated virtualisation solutions, shown as **option D**. These differ from option C in the way that a common orchestration layer can potentially span all compute nodes of one data centre and hence offer the largest flexibility in terms of the assignment of functional applications to compute resources.

All afore mentioned options shall be considered as a non-exhaustive list of possible platform approaches. A joint OCORA/RCA collaboration has initiated discussions regarding synergies between the CCS On-Board computing platform and the RCA track-side safe data centre.

In a first step, the group has compiled a whitepaper [19] and a set of high-level requirements [20]. In a second step industry discussions were conducted to narrow down the most promising platform approaches as well as to evaluate the concept of having a common unified platform independent API for On-Board and track-side functional applications. Subsequent the whitepaper [19] as well as the set of high-level requirements [20] have been adjusted based on the feedback received from the industry. The third step will once more involve the industry in defining a first version of the Platform Independent API.

10 Cyber security

Advancing inter-component communication increases the number of interfaces and points of contact between systems that are required for a state-of-the-art railway operation. Currently, there are no adequate and commonly used security solutions in place to protect against unauthorized access and to prevent unauthorized interventions and attacks. This results in a steadily growing vulnerability to internal and external attacks on safety-relevant systems of a railway operator.

Therefore, OCORA is required to consider security aspects of CCS On-Board solutions as well. Within a new European cooperation, security experts are developing harmonized security processes, strategies, and concepts.

The two main objectives of OCORA cyber security for this Release was the creation of an adequate security engineering process and the integration of (cyber-) security thoughts into the OCORA architecture e.g., zoning, principles, and levels (refer to Chapter B5 of Appendix B for the discussion about the different network topologies and zoning models).

OCORA Cyber Security collaborates and uses opinions/results from other security work groups.

Further information on cyber security is published in document [17] and [28]. The cyber security topic will be discussed in more detail in subsequent versions of the OCORA documents and with other relevant Cyber-security platforms like ER-ISAC and UIC P666 project.

Appendix A Train integration scenarios

OCORA has identified the following scenarios for integrating the OCORA CCS On-Board solution into the various type of trains. The scenarios listed are not exhaustive but provide a representative selection.

A1 Scenario A: CCN as physically separated network

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The CCS-, NG-TCN-, Communication- and Operator networks are physically separated networks interconnected through an ECN/ECN Security Gateway. This scenario further assumes that all Peripheral Devices are OCORA compliant and are therefore directly connected to the CCN, following the OCORA interface standard. Refer to Appendix B for further details on related topology of this scenario.

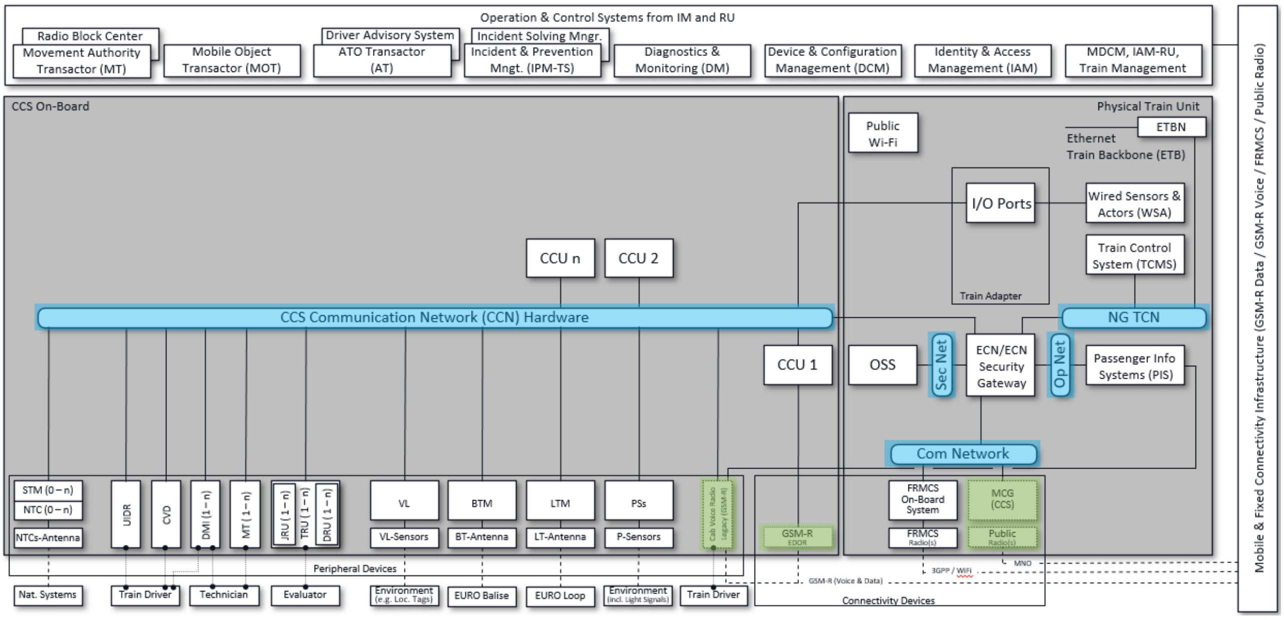

Figure 21 NG-TCN train – separate networks

Highlighted elements in Figure 21:

- Indication of physical segmentation between CCS, Train and other networks
- Components supporting legacy trackside infrastructure during migration phases

A2 Scenario B: CCN as logically separated network

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The control system networks (CCN and NG-TCN) are using the same physical network while separated from the non-control networks (e.g., Operator Network) through the ECN/ECN Security Gateway. The common control system network is then logically segmented into different virtual networks (VLANs) based on its **functional domain** (CCS and TCMS systems). This scenario further assumes that all peripheral devices and connectivity devices are OCORA compliant and are therefore directly connected to the CCN, following the OCORA interface standard. Refer to Appendix B for further details on related topology of this scenario.

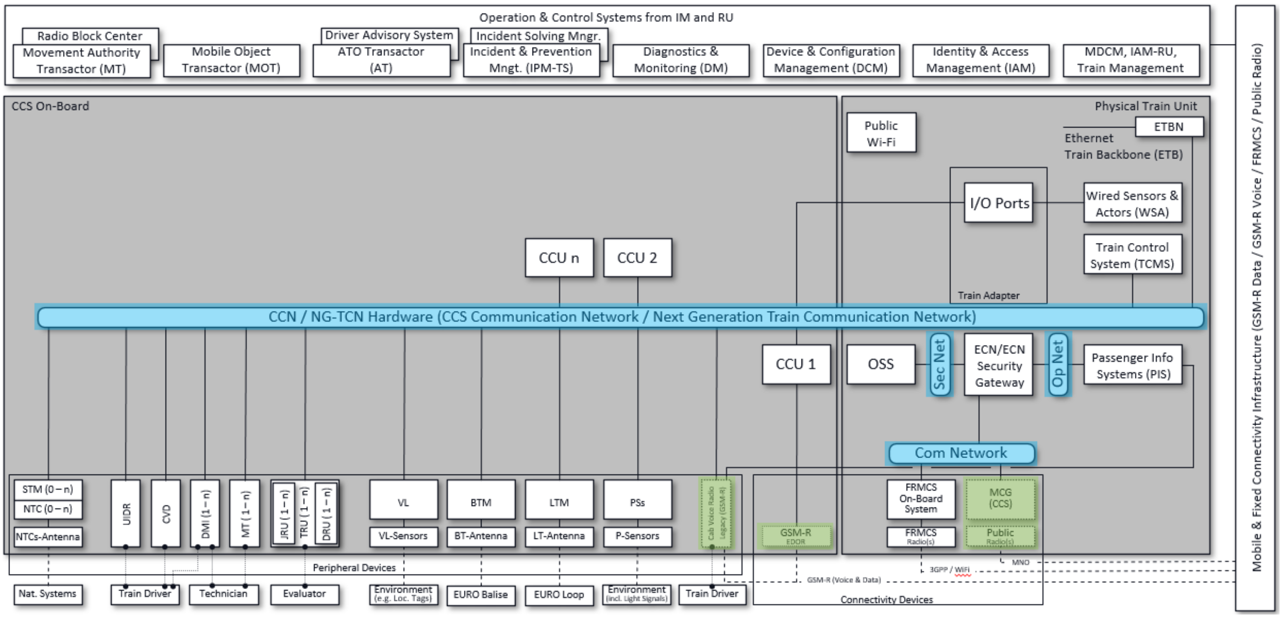

Figure 22 NG-TCN train – common network

Highlighted elements in Figure 22:

- Common physical network for the CCS and TCMS systems separated from non-control systems
- Components supporting legacy trackside infrastructure during migration phases

A3 Scenario C: Common critical control network logically separated

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The control system networks (CCN and NG-TCN) are using the same physical network while separated from the non-control networks (e.g., Operator Network) through the ECN/ECN Security Gateway. The common control system network is then logically segmented into different virtual networks (VLANs) based on its **criticality** (critical and non-critical control systems). This scenario further assumes that all peripheral devices and connectivity devices are OCORA compliant and are therefore directly connected to the CCN, following the OCORA interface standard. Refer to Appendix B for further details on related topology of this scenario.

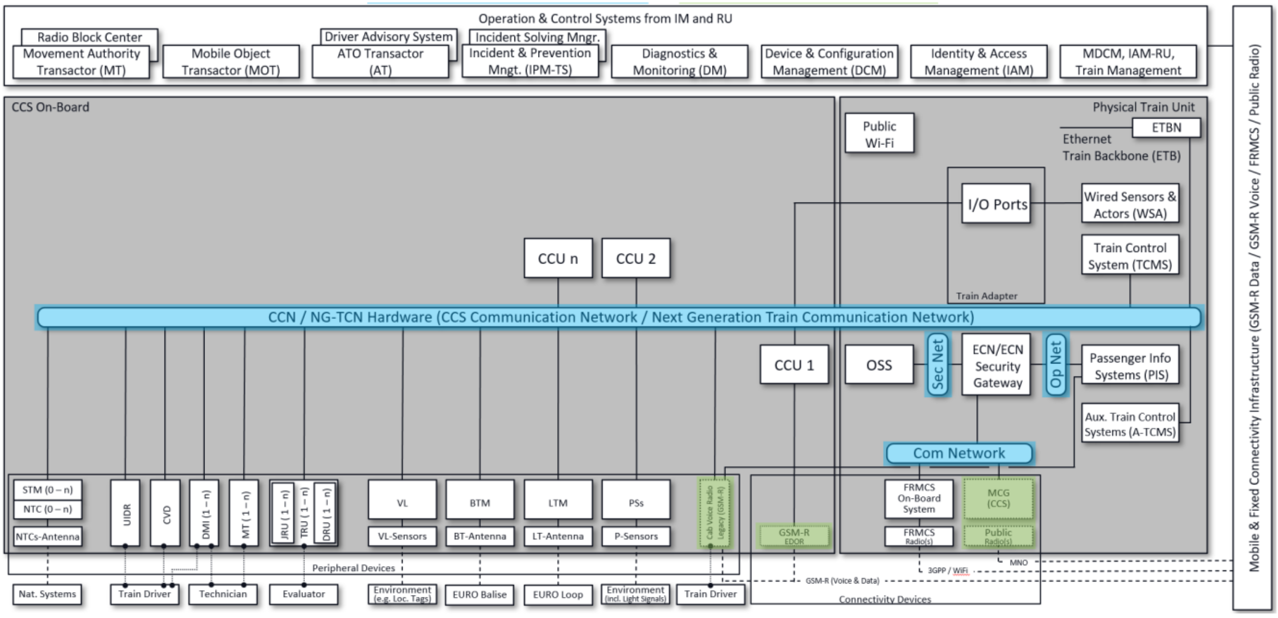

Figure 23 NG-TCN train – Common critical control network logically separated

Highlighted elements in Figure 23:

(blue)	Common physical network for the CCS and TCMS systems separated from non-control systems
(green)	Components supporting legacy trackside infrastructure during migration phases

A4 Scenario D: Common critical control network physically separated

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The critical-control systems (CCS and critical control components of the TCMS) are using the same physical network while physically separated from any other network (e.g., Operator network, Auxiliary network) through the ECN/ECN Security Gateway. This scenario further assumes that all peripheral devices and connectivity devices are OCORA compliant and are therefore directly connected to the CCN, following the OCORA interface standard. Refer to Appendix B for further details on related topology of this scenario.

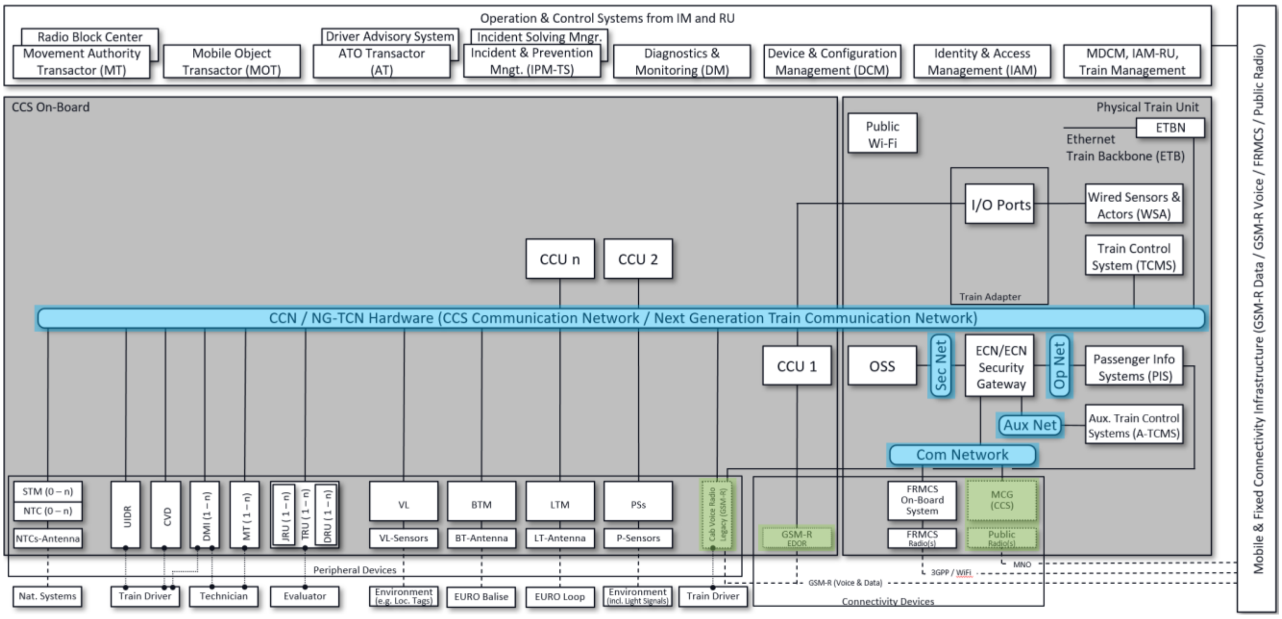

Figure 24 NG-TCN train – Common critical control network physically separated

Highlighted elements in Figure 24:

(blue)	Common physical network for the critical control systems separated from other networks
(green)	Components supporting legacy trackside infrastructure during migration phases

A5 Scenario for retrofit vehicles with OCORA compliant CCS peripherals

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a legacy train that has no Ethernet based network for its train control. Hence, the communication with the TCMS is implemented through the OCORA Gateway and the respective Functional Vehicle Adapter (FVA). This scenario further assumes that all Peripheral Devices and Connectivity Devices are OCORA compliant and are therefore directly connected to the CCN, following the OCORA interface standard. Refer to Appendix B for further details.

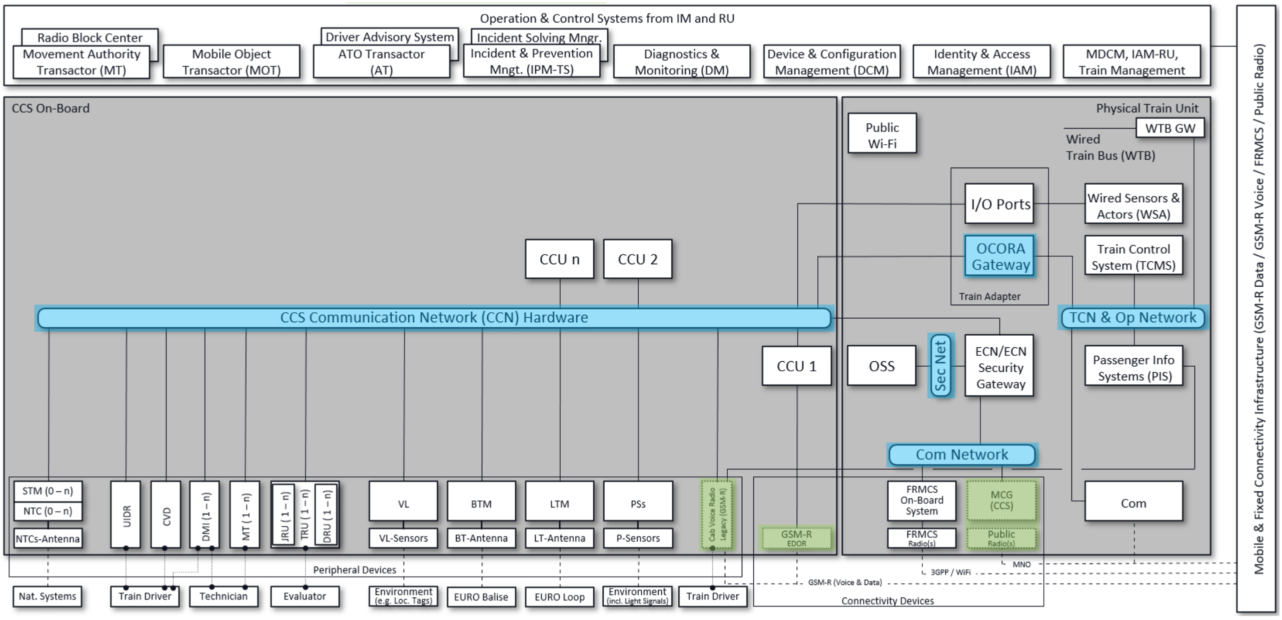

Figure 25 Legacy train – OCORA compliant CCS-OB peripherals

Highlighted elements in Figure 25:

Components related to the integration between the CCS and Train

Components supporting legacy trackside infrastructure during migration phases

Appendix B CCS On-Board – network topology scenarios

This appendix provides the updated ideas for the CCS On-Board network topology, including an updated set of scenarios to interconnect the different On-Board networks. These scenarios are the basis for further discussions about network architecture and cyber security and will be adapted as the architecture evolves.

B1 Scenario A: CCN as physically separated network

In this scenario, the CCN and the NG-TCN are physically separated. All communication components, all operator components and all security devices are located also on their own physically separated network. The network with connected public devices (e.g., public WLAN access point with connected passenger devices) is physically isolated. Every network represents a security zone.

The central element between all networks is the ECN/ECN Security Gateway (GW). The ECN/ECN Security Gateway routes the traffic between the different networks and acts as firewall between them. Cyber security aspects between trackside and onboard networks are covered in the FRMCS onboard system and MCG.

With the CCN as a physically separated network, the CCS and the TCMS domain are strictly divided. However, the complexity of the network configuration (TSN schedule) will increase due to the two separated network configurations linked together. And as the two network configurations of the two domains will be done independently the hard-real-time behavior for data between the two domains will suffer (latency and jitter will increase).

In the following two figures the physical and logical network architecture of scenario A is shown.

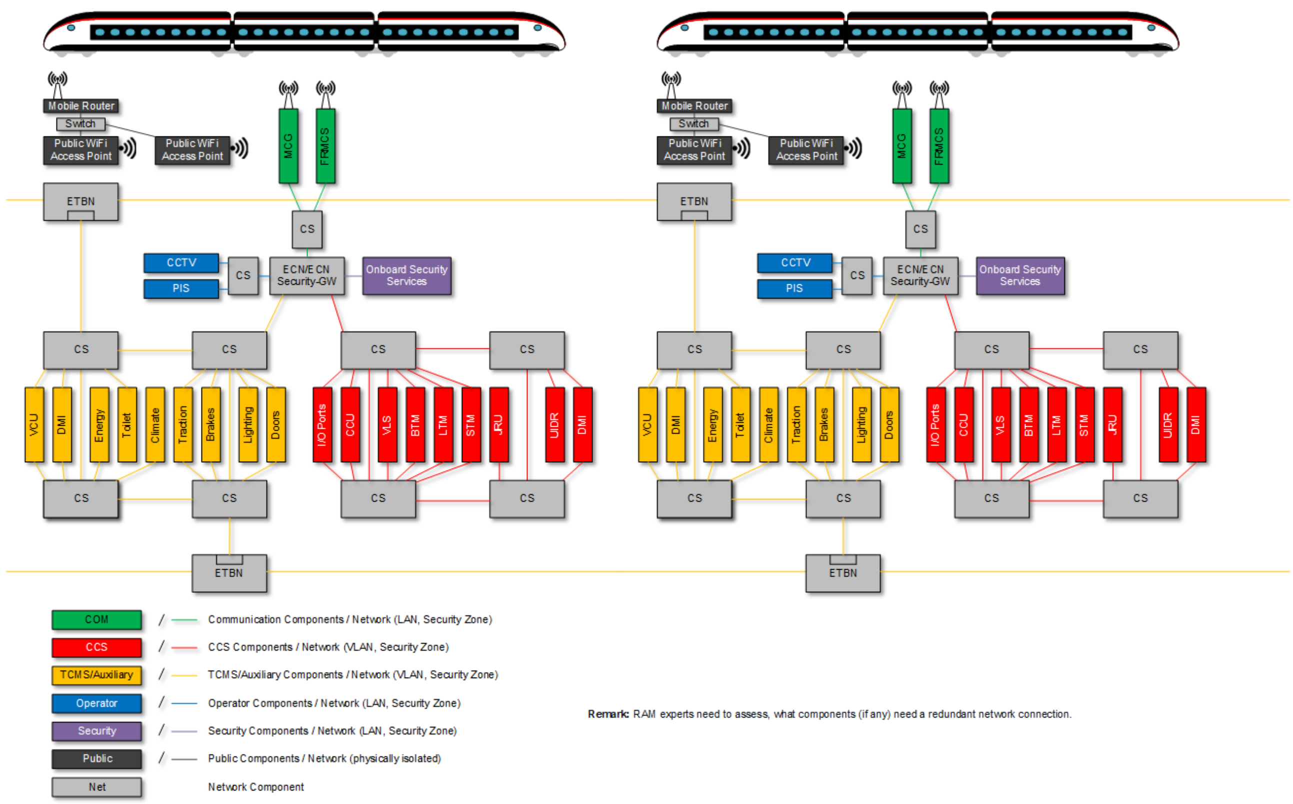

Figure 26 Physical network architecture scenario A: CCN as physically separated network

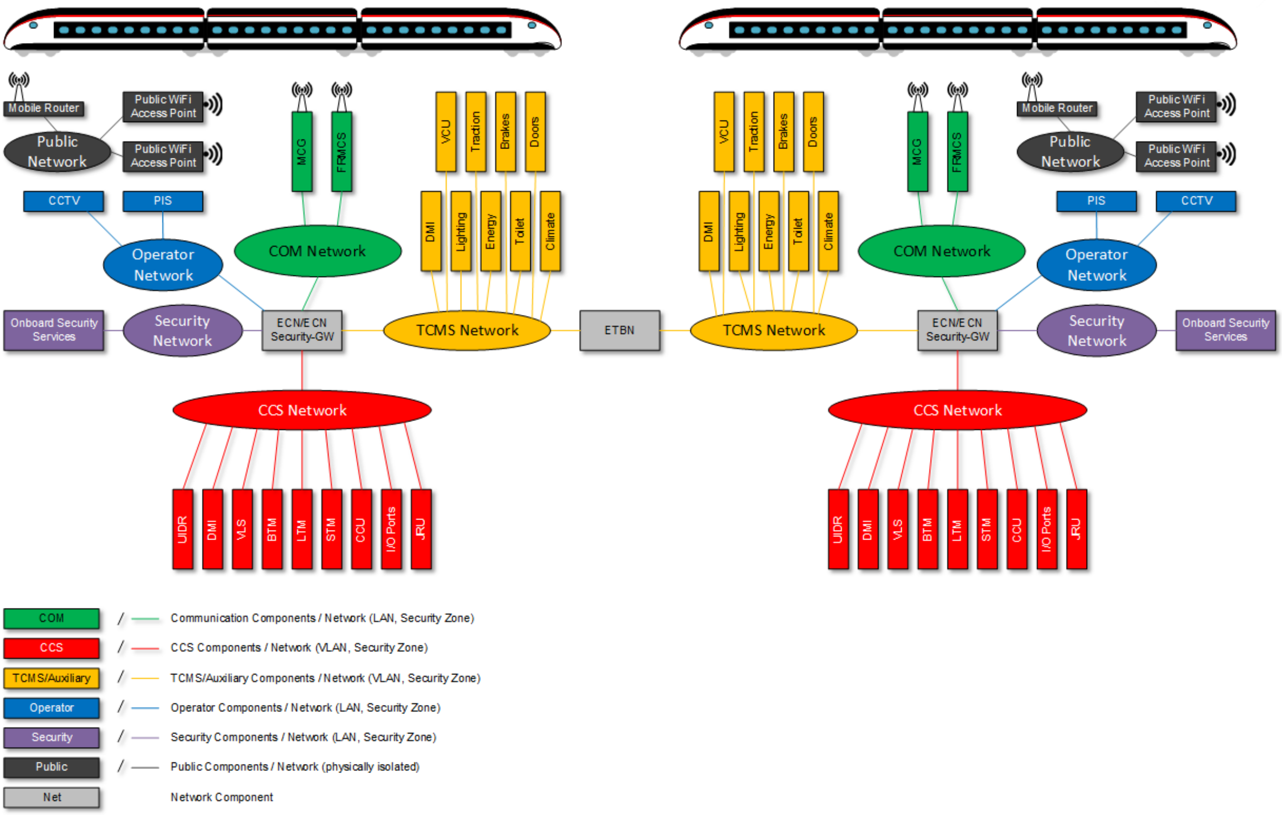

Figure 27: Logical network architecture scenario A: CCN as physically separated network

B2 Scenario B: CCN as logically separated network

In this scenario, the CCN and the NG-TCN are located on the same physical network. But the CCN and NG-TCN are logically separated. So, the CCN and the NG-TCN represent an own logical network. All communication components, all operator components and all security devices are located on their own physically separated network. The network with connected public devices (e.g., public WLAN access point with connected passenger devices) is physically isolated. Every logical network represents a security zone.

The central element between all networks is the ECN/ECN Security Gateway (GW). The ECN/ECN Security Gateway routes the traffic between the different networks and acts as firewall between them. Cyber security aspects between trackside and onboard networks are covered in the FRMCS onboard system and MCG.

With the CCN as a logically separated network, the CCS and the TCMS domain are strictly divided. The complexity of the network configuration (TSN schedule) is low due to the fact of having only one network configuration for the common physical network (CCN and NG-TCN). The hard-real-time behavior for data between the two domains over the ECN/ECN Gateway is sufficient.

In the following two figures the physical and logical network architecture of scenario B is shown.

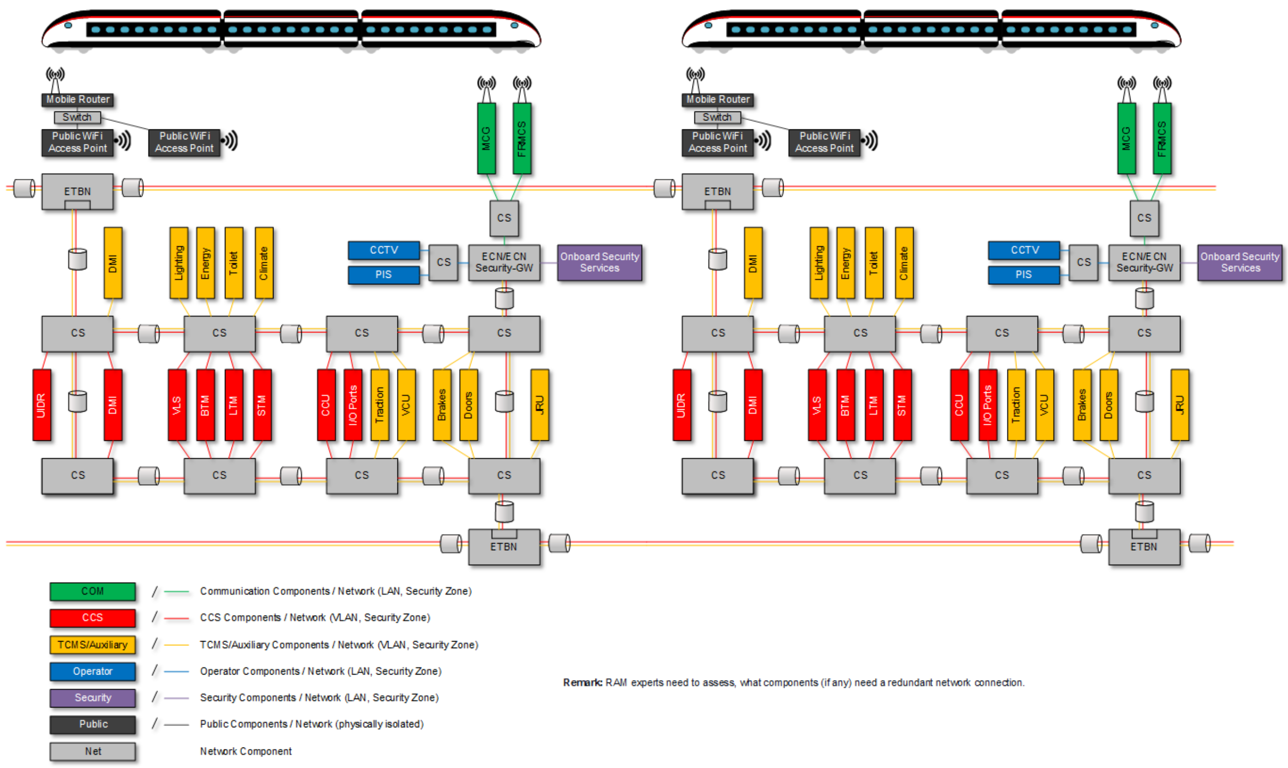

Figure 28 Physical network architecture scenario B: CCN as logically separated network

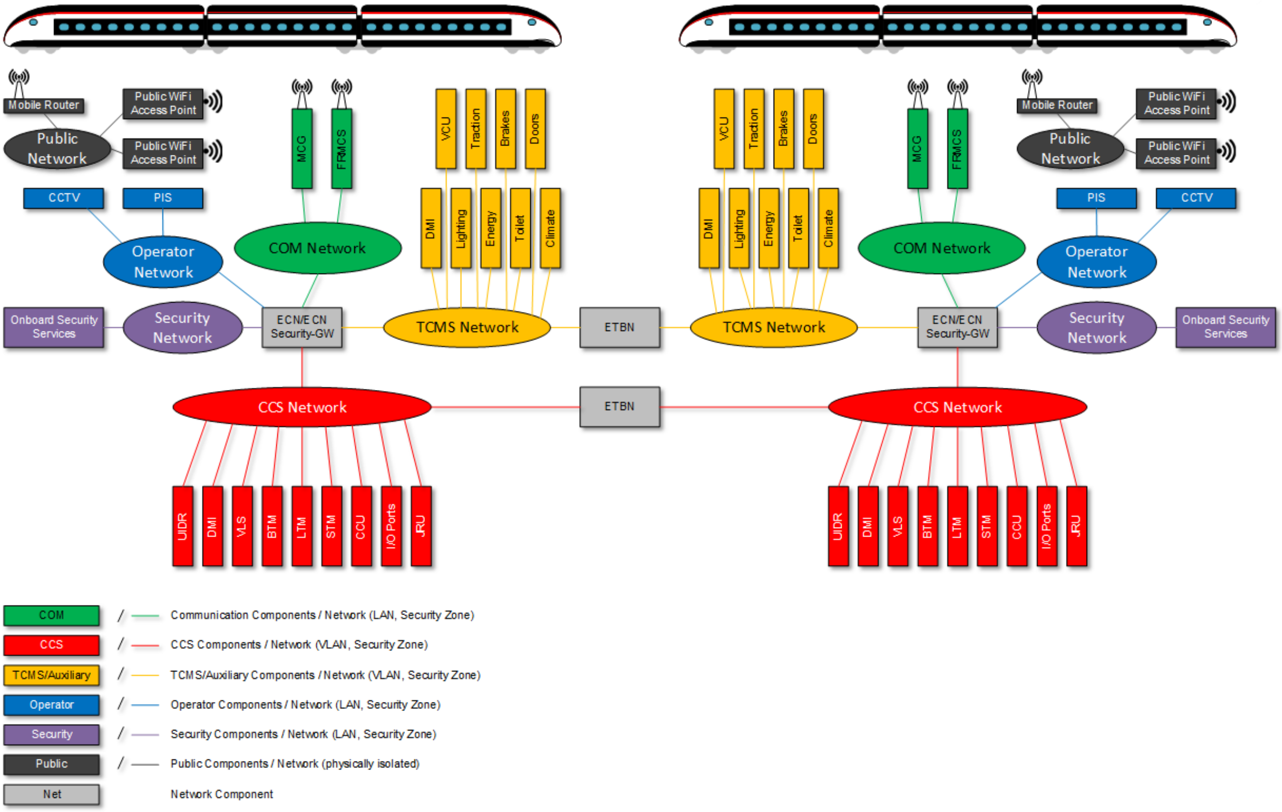

Figure 29: Logical network architecture scenario B: CCN as logically separated network

B3 Scenario C: Common critical control network logically separated

In this scenario, the networks or security zones are derived from the criticality of the functions of the train. The CCS components and the critical control components of the TCMS domain (e.g., VCU, Traction, Brakes, Doors) are located on the same logical network. The non-critical control components of the TCMS domain, the auxiliary components, like e.g., toilets, climate and lighting are located in a logically separated network on the same physical network together with the critical control components. So, the CCS/TCMS and the auxiliary network represent an own logical network. The detailed split of the TCMS domain into a critical and a non-critical part should be defined by the TCMS sector (e.g., CONNECTA, X2Rail). All communication components, all operator components and all security devices are located on their own physically separated network. The network with connected public devices (e.g., public WLAN access point with connected passenger devices) is physically isolated. Every logical network represents a security zone.

The central element between all networks is the ECN/ECN Security Gateway (GW). The ECN/ECN Security Gateway routes the traffic between the different networks and acts as firewall between them. Cyber security aspects between trackside and onboard networks are covered in the FRMCS onboard system and MCG.

In this scenario critical control systems are logically separated from non-critical control systems. The complexity of the network configuration (TSN schedule) is low due to the fact of having only one network configuration for the common physical network (CCN and NG-TCN). The hard-real-time behavior for data between the CCS domain and critical part of TCMS domain without a gateway in between is excellent (very low latency and jitter in µs and ns range).

In the following two figures the physical and logical network architecture of scenario C is shown.

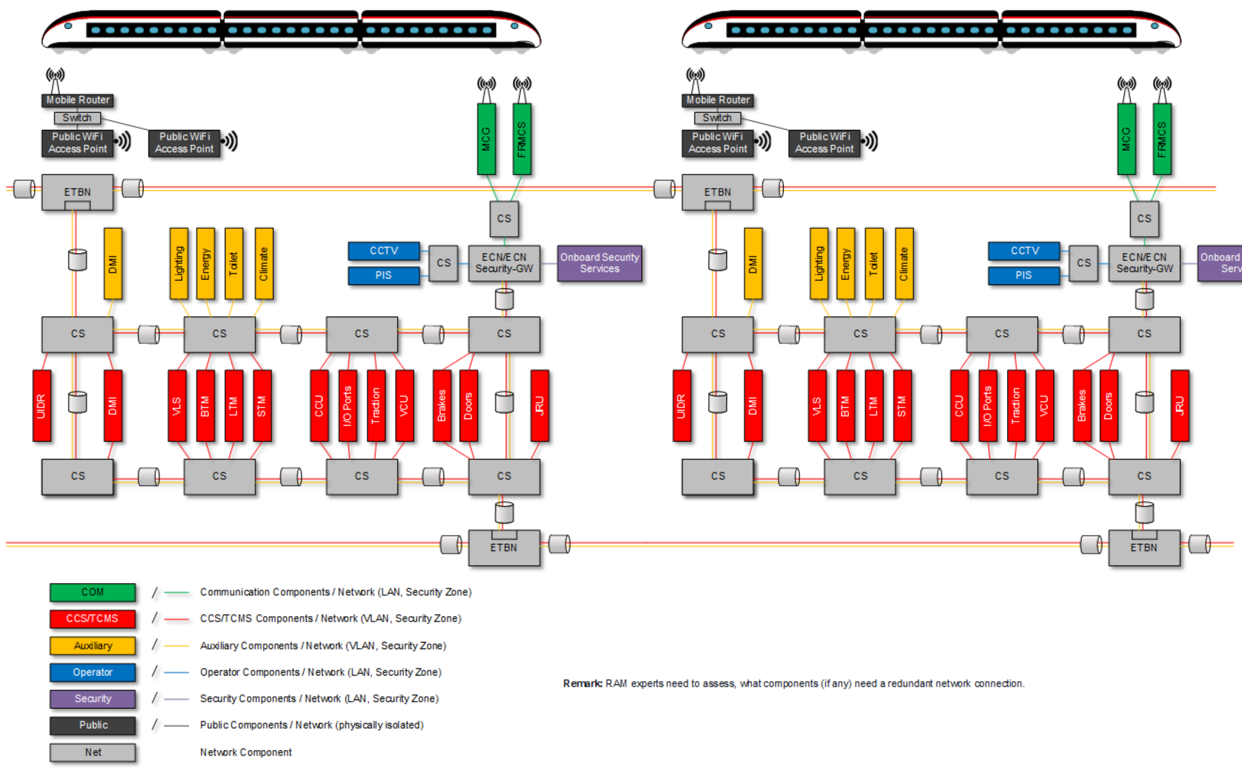

Figure 30 Physical network architecture scenario C: Common critical control network logically sep.

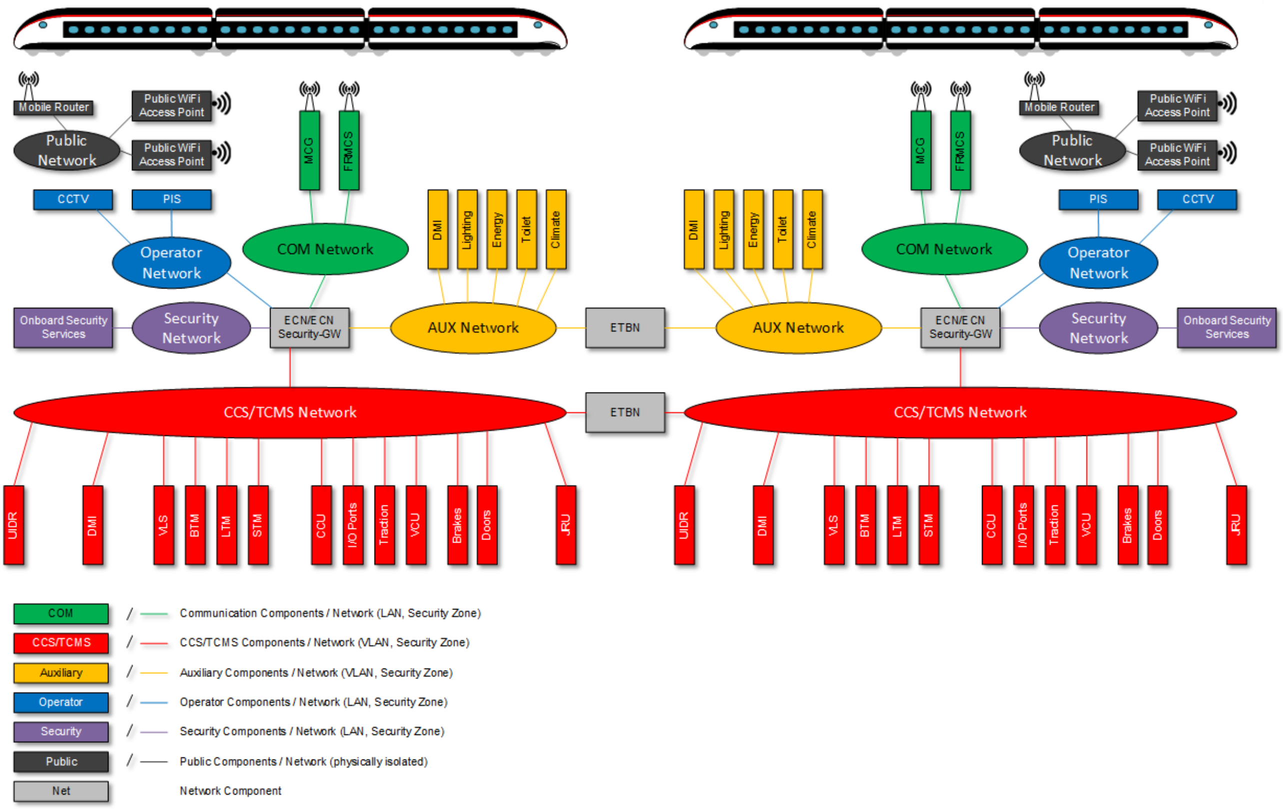

Figure 31: Logical network architecture scenario C: Common critical control network logically sep.

B4 Scenario D: Common critical control network physically separated

In this scenario, the networks or security zones are derived from the criticality of the functions of the train. The CCS components and the critical control components of the TCMS domain (e.g., VCU, Traction, Brakes, Doors) are located on the same logical network. The non-critical control components of the TCMS domain, the auxiliary components, like e.g., toilets, climate and lighting are located in an own physically separated network. The detailed split of the TCMS domain into a critical and a non-critical part should be defined by the TCMS sector (e.g., CONNECTA, X2Rail). All communication components, all operator components and all security devices are located on their own physically separated network. The network with connected public devices (e.g., public WLAN access point with connected passenger devices) is physically isolated. Every logical network represents a security zone.

The central element between all networks is the ECN/ECN Security Gateway (GW). The ECN/ECN Security Gateway routes the traffic between the different networks and acts as firewall between them. Cyber security aspects between trackside and onboard networks are covered in the FRMCS onboard system and MCG.

In this scenario critical control systems are physically separated from non-critical control systems. The complexity of the network configuration (TSN schedule) is high due to the fact of having two network configurations for the two physical networks CCS/TCMS and Auxiliary. The hard-real-time behavior for data between the CCS domain and critical part of TCMS domain without a gateway in between is still excellent (very low latency and jitter in µs and ns range).

In the following two figures the physical and logical network architecture of scenario D is shown.

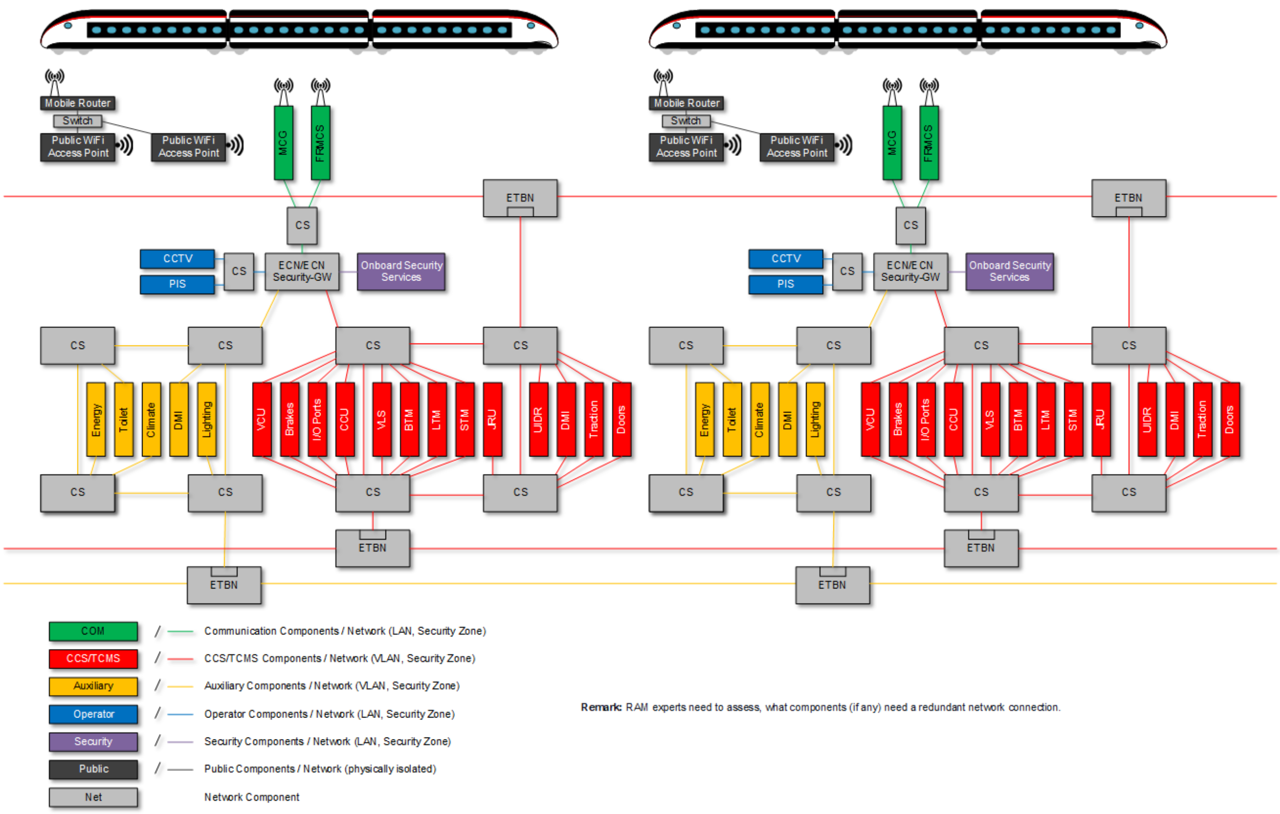

Figure 32: Physical network architecture scenario D: Common critical control network physically sep.

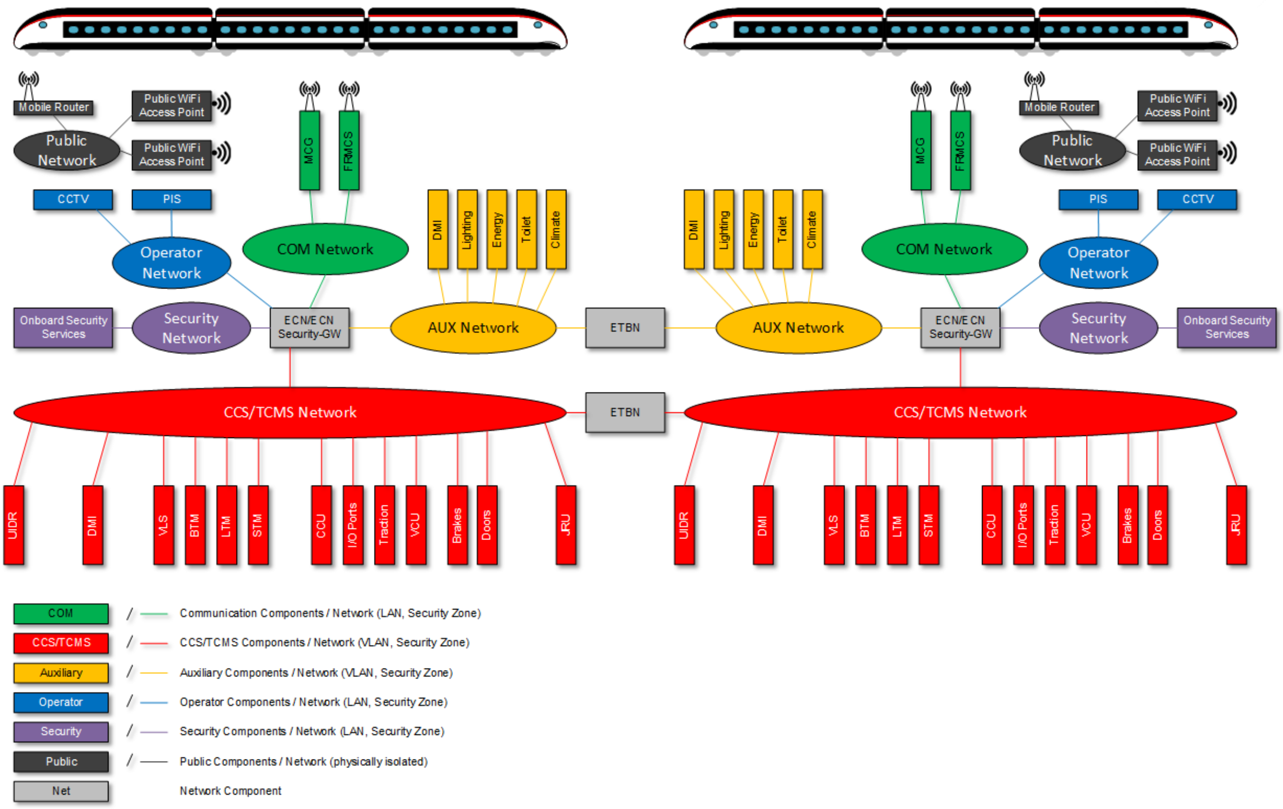

Figure 33: Logical network architecture scenario D: Common critical control network physically sep.

B5 Evaluation network architecture scenarios for new trains

Table 26 gives an overview on the advantages and disadvantages of the different evaluated network architectures for new trains.

Network Architecture for new Trains	Advantage	Disadvantage
Scenario A: CCN as physically separated network (Figure 26, Figure 27)	- Clear physical separation between CCS and TCMS domain. - Consist switches are not security relevant.	- No clear separation between critical control systems and non-critical control systems - Complex network configuration (e.g., for hard-real-time traffic between CCS and TCMS domain) - No direct communication between CCS and TCMS possible. Therefore, bad hard-real-time behavior. - No direct inter-consist communication for CCS
Scenario B: CCN as logically separated network (Figure 28, Figure 29)	- Clear logical separation between CCS and TCMS domain - Direct inter-consist communication for CCS possible	- No clear separation between critical control systems and non-critical control systems - No direct communication between CCS and TCMS possible. - Consist switches responsible for the logical segmentation become security relevant and have to meet certain requirements.
Scenario C: Common critical control network logically separated (Figure 30, Figure 31)	- Clear separation of critical control systems and non-critical control systems - Direct communication between all critical control devices of any domain possible. - Excellent hard-real-time behavior ensures deterministic communication. - Direct inter-consist communication for CCS possible	- No clear separation between CCS and TCMS domain. - Consist switches responsible for the logical segmentation become security relevant and have to meet certain requirements.
Scenario D: Common critical control network physically separated (Figure 32, Figure 33)	- Clear separation of critical control systems and non-critical control systems - Direct communication between all critical control devices of any domain possible. - Excellent hard-real-time behavior ensures deterministic communication. - Consist switches are not security relevant.	- Complex network configuration (e.g., for hard-real-time traffic between CCS/TCMS and Auxiliary systems) - No clear separation between CCS and TCMS domain. - Direct inter-consist communication for auxiliary systems only with additional train routers and train line possible.

Table 26: Overview of network architectures for new trains

Further details of the evaluation of the different network architecture scenarios can be found in the OCORA CCN Evaluation report [17].

B6 Network architecture for retrofit vehicles

Current TCN layouts differ between vehicle manufacturers. Especially the consist networks and technologies including the used network protocols are often proprietary implementations of the manufactures. The network architecture of retrofit vehicles will be vehicle dependent and therefore project specific.

The legacy and much standardized combination of WTB and MVB is still used for the TCMS. But the need for larger usable data bandwidth led to diverse network implementations where several TCMS busses or networks coexist. Today, within consists at least these network protocols are used:

- MVB & WTB (for TCMS, legacy)
- CAN (for local subsystems, e.g., Boogie Control)
- PROFIBUS (Siemens, legacy)
- Profinet (Ethernet, Siemens)
- CIP (Ethernet, Alstom)
- IPTCom (Ethernet, Bombardier)
- TRDP (Ethernet, Stadler, Bombardier, Toshiba, Siemens, CAF)

In the legacy train the network of the TCMS normally will not change. So, the CCN must establish its own ECN network for CCS devices only. The CCN and the legacy TCN are therefore physically separated. The CCN is connected to the legacy TCN over the OCORA Gateway (GW). All communication components, all operator components and all security devices are located also on their own physically separated network. The network with connected public devices (e.g., public WLAN access point with connected passenger devices) is physically isolated. Every network represents a security zone.

In the following two figures an example a physical and a logical network architecture of retrofit scenario is shown. For simplicity only one TCMS bus is outlined.

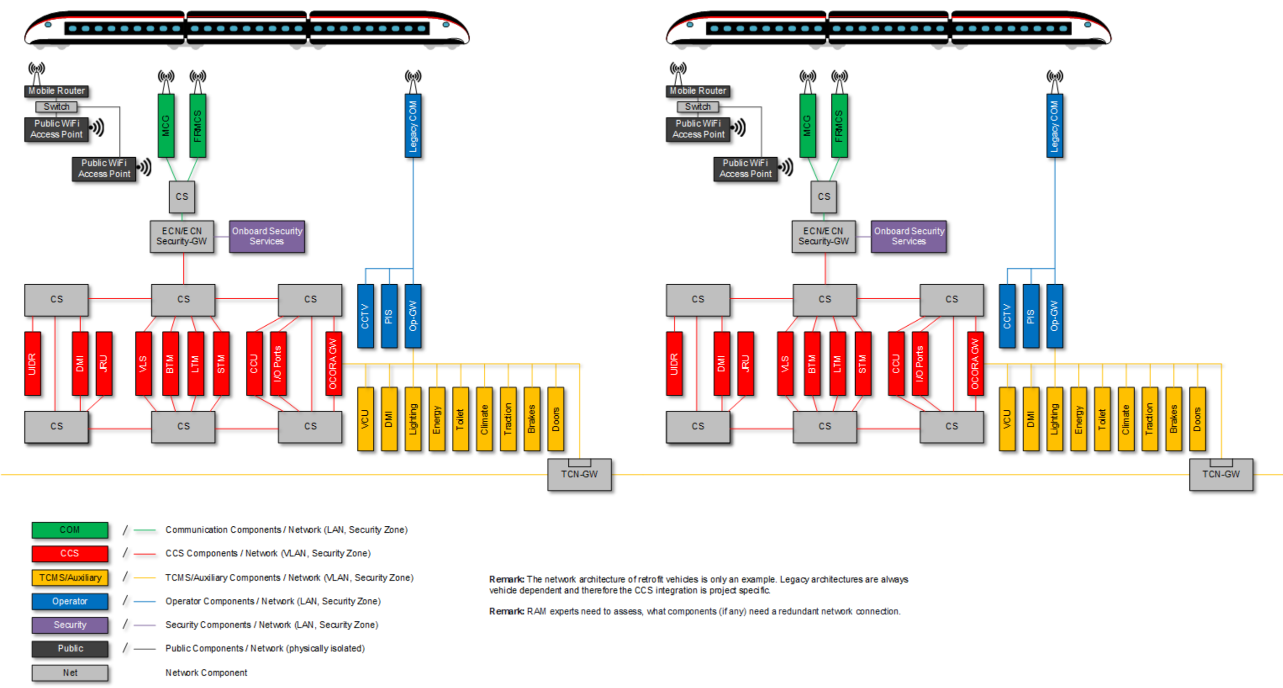

Figure 34: Physical network architecture scenario for retrofit vehicles

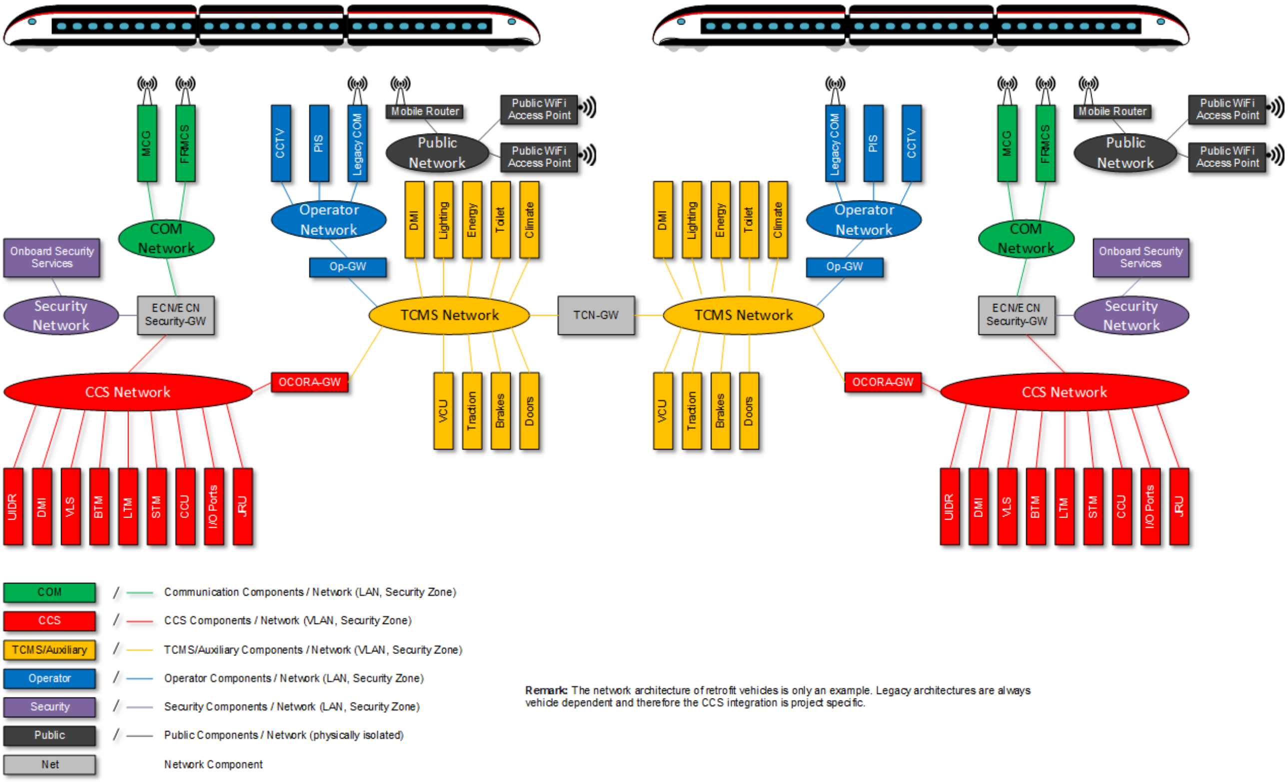

Figure 35: Logical network architecture scenario for retrofit vehicles

Appendix C Relating functions from SUBSET-026

To support modularity, OCORA suggests implementing the current ETCS On-Board functionality in separate functional blocks. Among others, the following key functional blocks have been already identified in previous OCORA releases: VS = Vehicle Supervisor / VL = Vehicle Locator / MLM = Mode & Level Manager / STMC = STM Control. This list of functional blocks has now evolved and do so in subsequent releases of the OCORA documentation releases.

The following table assigns current ETCS On-Board functionality (as per SUBSET-026, chapter 4.5) to the respective functional block. It contains, on a very high-level, a first proposed split of functionality between the functional block identified so far. The OCORA architecture team is aware that splitting the functionality only based on the SUBSET-026, chapter 4.5 is not sufficient, because the subset does not provide all requirements. SUBSET-026 is providing the mandatory requirement specifications only. A more detailed separation and identification of additional requirements to SUBSET-026 can be expected in subsequent OCORA documentation releases.

N°	On-Board Functions	Reference SUBSET-026	VS	VL	MLM	STMC	Standstill Detection	Cold movement Detection	NTC-APP	TCS	Physical ETCS transponder services	Operational Data Storage	Configuration data storage	FVA	Time service on-board	JRU message compiler	Train integrity Status Management	DMI
	Data Consistency																	
1)	Check linking consistency	3.16.2.3 3.4.4	X [1]															
2)	Check Balise Group Message Consistency if linking consistency is checked	3.16.2.4.1 3.16.2.4.3	X [1]															
3)	Check Balise Group Message Consistency if no linking consistency is checked (because no linking information is available and/or because the function "check linking consistency is not active)	3.16.2.4.4	X [1]															
4)	Check Unlinked Balise Group Message Consistency	3.16.2.5	X [1]															
5)	Check correctness of radio messages	3.16.3.1.1	X															
6)	Check radio sequence	3.16.3.3	X															
7)	Check safe radio connection (only level 2/3)	3.16.3.4	X															
	Determine Train Speed and Position																	
8)	Determine train position referenced to LRBG	3.6.1 3.6.4		X														
9)	Determine train speed, train acceleration	None		X														
10)	Determine train standstill						X											
11)	Determine Geographical Position	3.6.6	X	X [2]														
12)	Report train position when train reaches standstill	3.6.5.1.4 a)	X [3]															

[1] VS informs VL about valid Balise Groups
[2] In case of on-board localisation
[3] Content must be safe in future (L3 / moving block); Trigger for Report is "ns"

N°	On-Board Functions	Reference SUBSET-026	VS	VL	MLM	STMC	Standstill Detection	Cold movement Detection	NTC-APP	TCS	Physical ETCS transponder services	Operational Data Storage	Configuration data storage	FVA	Time service on-board	JRU message compiler	Train integrity Status Management	DMI
13)	Report train position when mode changes to...1	3.6.5.1.4 b)	X [4]															
14)	Report train position when train integrity confirmed by driver	3.6.5.1.4 c)	X [4]															
15)	Report train position when loss of train integrity is detected	3.6.5.1.4 d)	X [4]															
16)	Report train position when train front/rear passes an RBC/RBC border (only level 2/3)	3.6.5.1.4 e) 3.6.5.1.4 k)	X [4]															
17)	Report train position when train rear passes a level transition border (from level 2/3 to 0, NTC, 1)	3.6.5.1.4f)	X [4]															
18)	Report train position when change of level due to trackside order	3.6.5.1.4 g)	X [4]															
19)	Report train position when change of level due to driver request	3.6.5.1.4 g)	X [4]															
20)	Report train position when establishing a session with RBC	3.6.5.1.4 h)	X [4]															
21)	Report train position when a data consistency error is detected (only level 2/3)	3.6.5.1.4 i)	X [4]															
22)	Report train position as requested by RBC...	3.6.5.1.4	X [4]															
23)	... or Report train position at every passage of an LRBG compliant balise group	3.6.5.1.4 j)	X [4]															
	Manage MA																	
24)	Request MA Cyclically respect to approach of perturbation location (T_MAR) or MA timer elapsing (T_TIMEOUTRQST) (only level 2/3)	3.8.2.3 a) and b)	X															
25)	Request MA Cyclically when “Start” is selected (only level 2/3)	4.4.11 5.4, 5.11	X															
26)	Request MA on reception of "track ahead free up to the level 2/3 transition location" (only level 0,1,NTC)	3.8.2.7.1	X															
27)	Request MA on track description deletion (only level 2/3)	3.8.2.7.3	X															
28)	Determine EOA/LOA, SvL, Danger Point, etc...	3.8.4 3.8.5	X															
29)	Handle Co-operative MA revocation (only level 2/3)	3.8.6	X															
30)	Manage Unconditional Emergency Stop	3.10	X															
31)	Manage Conditional Emergency Stop	3.10	X															
	Determine Most Restrictive Speed Profile, based on:																	
32)	SSP	3.11.3	X															
33)	ASP	3.11.4	X															
34)	TSR	3.11.5	X															

N°	On-Board Functions	Reference SUBSET-026	VS	VL	MLM	STMC	Standstill Detection	Cold movement Detection	NTC-APP	TCS	Physical ETCS transponder services	Operational Data Storage	Configuration data storage	FVA	Time service on-board	JRU message compiler	Train integrity Status Management	DMI
35)	Signalling related speed restriction when evaluated as a speed limit	3.11.6	X															
36)	Mode related speed restriction	3.11.7	X															
37)	Train related speed restriction	3.11.8	X															
38)	STM max speed	3.11.2.2 g)	X															
39)	STM system speed	3.11.2.2 h)	X															
40)	LX speed	3.12.5.6	X															
41)	Speed restriction to ensure a given permitted braking distance	3.11.11	X															
42)	Override related speed restriction	5.8.3.6	X															
	Supervise Train Speed																	
43)	Speed and Distance Monitoring based on MRSP, MA, release speed, gradient, mode profile, non-protected LX start location, and route unsuitability location	3.13 5.9.3.5 57.3.4 3.12.2.8 3.12.5.4	X															
44)	Speed and Distance Monitoring based on MRSP	4.4.10.1	X															
45)	Speed and Distance Monitoring based on MRSP, allowed distance to run in Staff Resp. mode	4.4.11	X															
46)	Ceiling Speed Monitoring only (no braking curve) based on MRSP	4.4.8.1.1 a) 4.4.18.1.3 a)	X															
	Supervise Train Movements																	
47)	Backwards Distance Monitoring	4.4	X															
48)	Roll Away Protection	3.14.2	X															
49)	Reverse Movement Protection	3.14.3	X															
50)	Standstill Supervision	3.14.4 4.4.7.1.5	X															
51)	Supervise “danger for shunting” information and list of expected balises for shunting	4.4.8.1.1 b) and c)	X															
52)	Supervise “Stop if in SR” information and list of expected balises for Staff Responsible	4.4.11.1.3 c) and d)	X															
53)	Supervise signalling related speed restriction when evaluated as a trip order	3.11.6.4	X															
54)	Command Emergency Brake	4	X		tbd				X									
55)	**Determine Mode and Level**																	
56)	Determine ERTMS/ETCS Mode	3.12.4 4.6			X													
57)	Determine ERTMS/ETCS level	5.10			X													
58)	**Other functions**																	
59)	System Version Management	3.17	X															

N°	On-Board Functions	Reference SUBSET-026	VS	VL	MLM	STMC	Standstill Detection	Cold movement Detection	NTC-APP	TCS	Physical ETCS transponder services	Operational Data Storage	Configuration data storage	FVA	Time service on-board	JRU message compiler	Train integrity Status Management	DMI
60)	Manage Communication Session	3.5	X [4]															
61)	Delete Revoked TSR	3.11.5.5	X															
62)	Override (Trip inhibition)	5.8	X															
63)	Manage Track Conditions excluding Sound Horn, Non-Stopping Areas, Tunnel Stopping Areas and Big Metal Masses	3.12.1	X							X								
64)	Manage Track Conditions Sound Horn, Non-Stopping Areas, Tunnel Stopping Areas	3.12.1	X															
65)	Manage Track Condition Big Metal Masses	3.12.1	X								X ?							
66)	Manage Route Suitability	3.12.2	X															
67)	Manage Text Display to the driver	3.12.3	X (and DMI?)															
68)	Manage LSSMA display to the driver	4.4.19.1	X (and DMI?)															
69)	Manage RBC/RBC Handover (only level 2/3)	3.15.1 5.15	X [5]															
70)	Manage Track Ahead Free Request (only level 2/3)	3.15.5	X															
71)	Provide Fixed Values, and Default/National Values	3.18.1 3.18.2	X									X						
72)	Manage change of Train Data from external sources	5.17	X										X	X				
73)	Provide Date and Time	3.18.5													X			
74)	Provide Juridical Data	3.20														X		
75)	Inhibition of revocable TSRs from balises (only level 2/3)	3.11.5.12 3.11.5.13 3.11.5.14 3.11.5.15	X															
76)	Cold Movement Detection	3.15.8						X										
77)	Continue Shunting on desk closure (Enabling transition to Passive Shunting mode)	5.12.4			X													
78)	Manage "Stop Shunting on desk opening" information	4.4.20.1.8 4.4.20.1.9			X													
79)	Manage Virtual Balise Covers	3.15.9	X															
80)	Advance display of route related information	3.15.10	X (and DMI?)															

Table 27 Relating Functions from SUBSET-026

[4] OCORA aims to split safe from non-safe functionality. Hence, it might be reasonable to remove this functionality from the VS and have it implemented in a separate component. This will be elaborated in more detail in subsequent versions of this document.
[5] RBC handover might also be relevant for VL, e.g. digital map downloads

Appendix D Large scale graphics

D1 Physical architecture for CCS-OB – actors and external interfaces

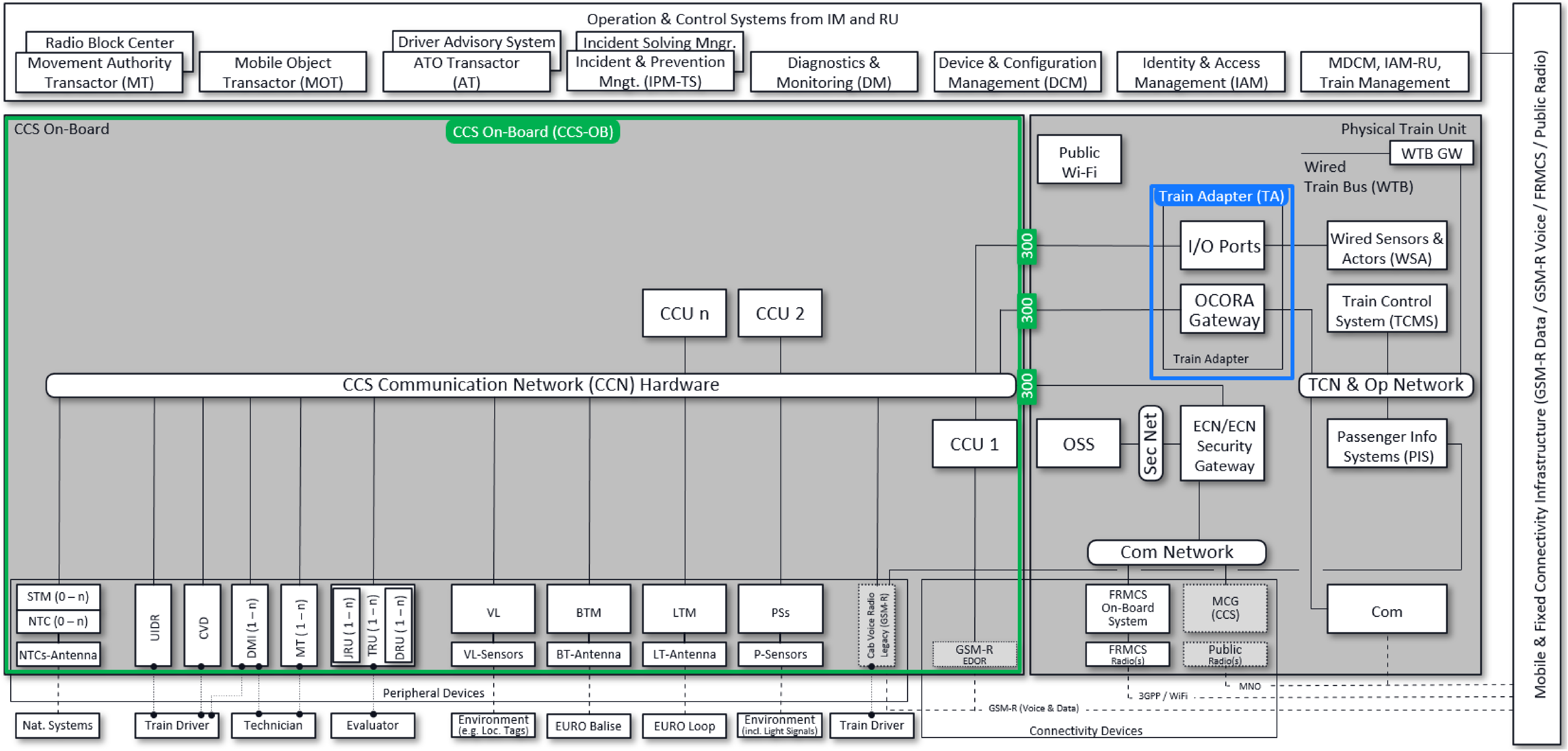

Figure 36 CCS-OB physical architecture – scope, actors, and external interface

D2 Physical architecture for CCS-OB – components and internal interfaces

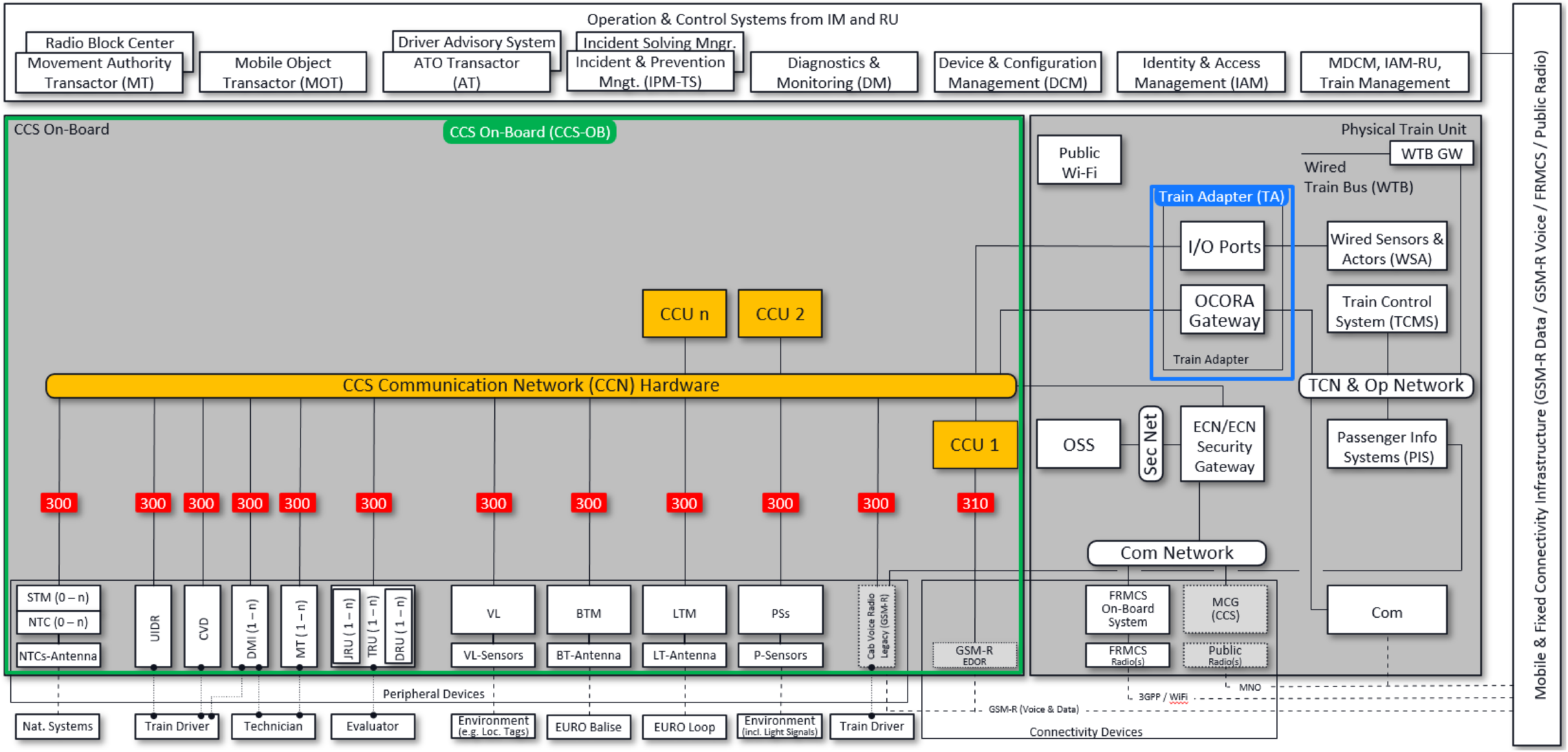

Figure 37 CCS-OB physical architecture – components and internal interface

D3 Logical architecture for CCS-OB – actors and external interfaces

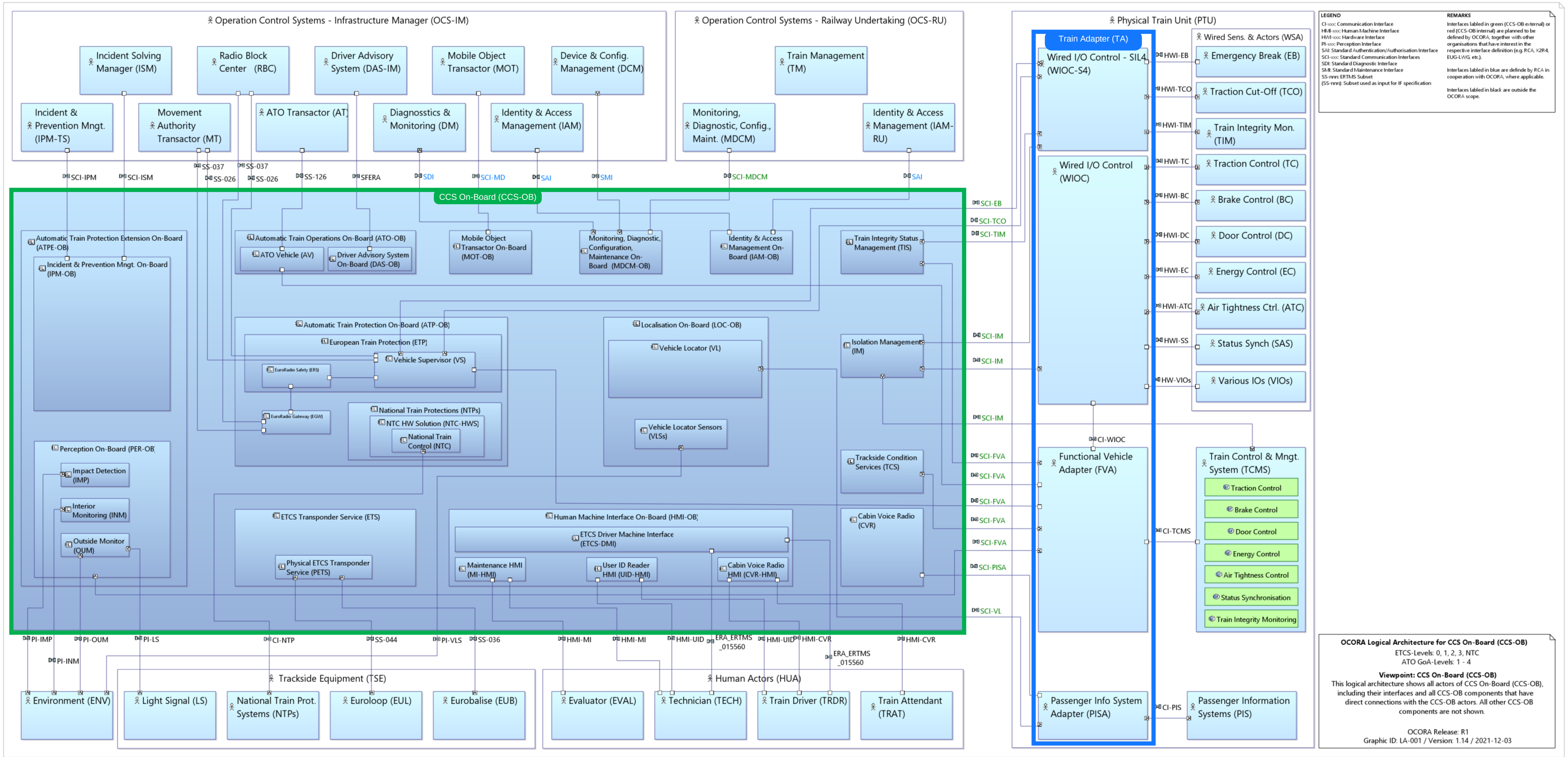

Figure 38 CCS-OB logical architecture – scope, actors, and external interfaces

D4 Logical architecture for CCS-OB – components and internal interfaces

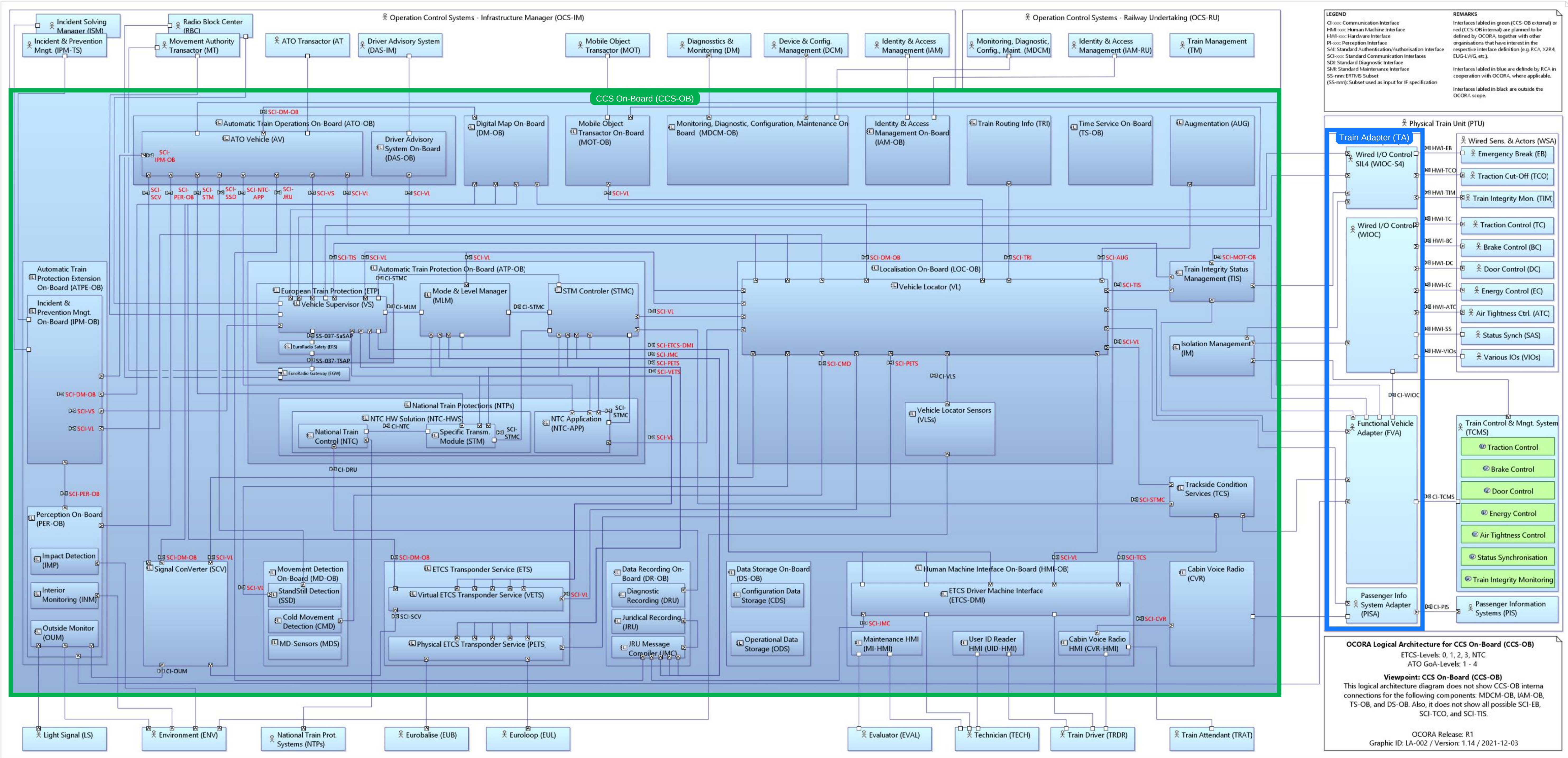

Figure 39 CCS-OB logical architecture – components and internal interfaces

D5 Logical architecture for CCS-OB – Viewpoint ATP-OB

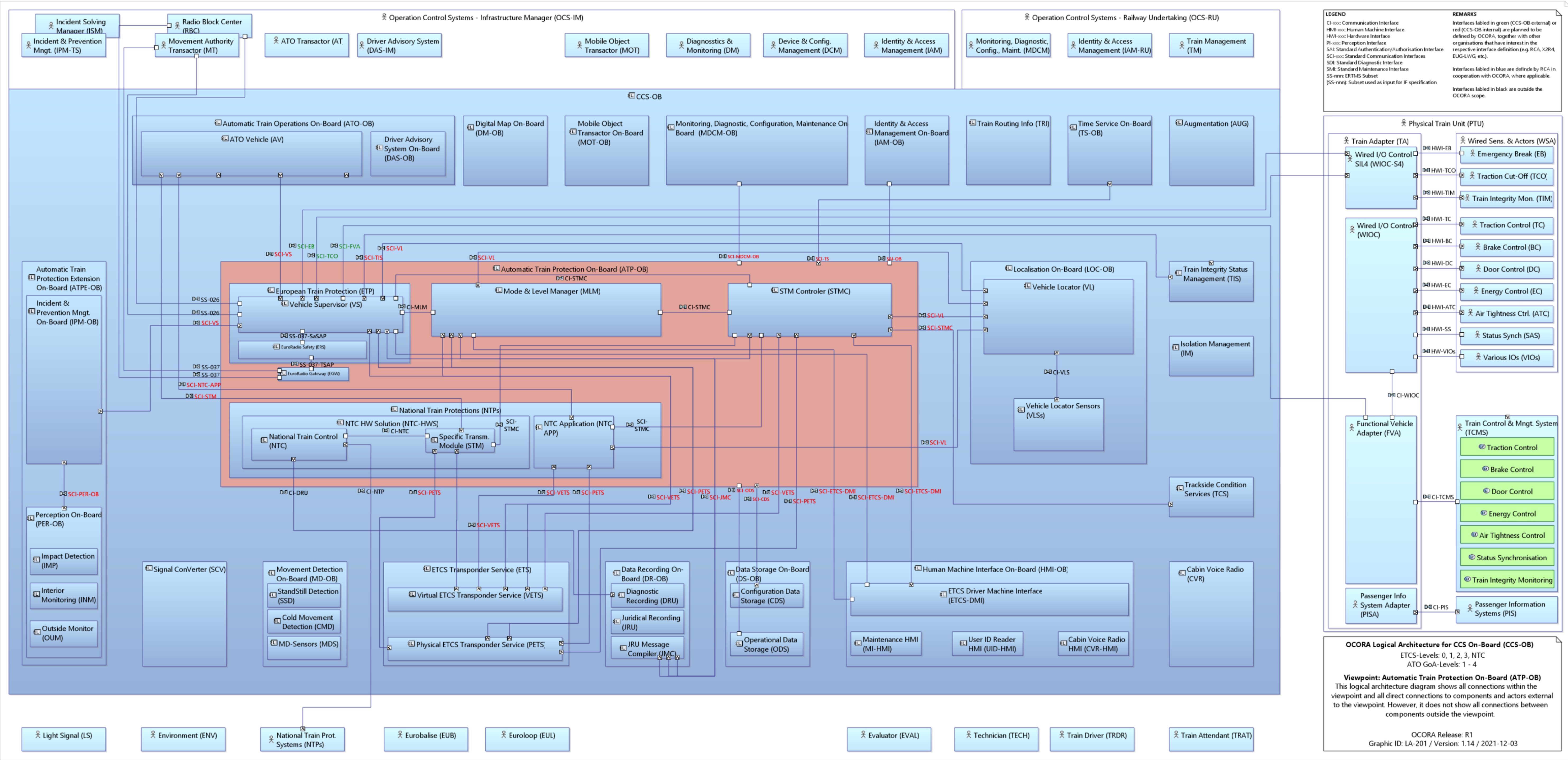

Figure 40 CCS-OB logical architecture – Viewpoint ATP-OB

D6 Logical architecture for CCS-OB – Viewpoint LOC-OB

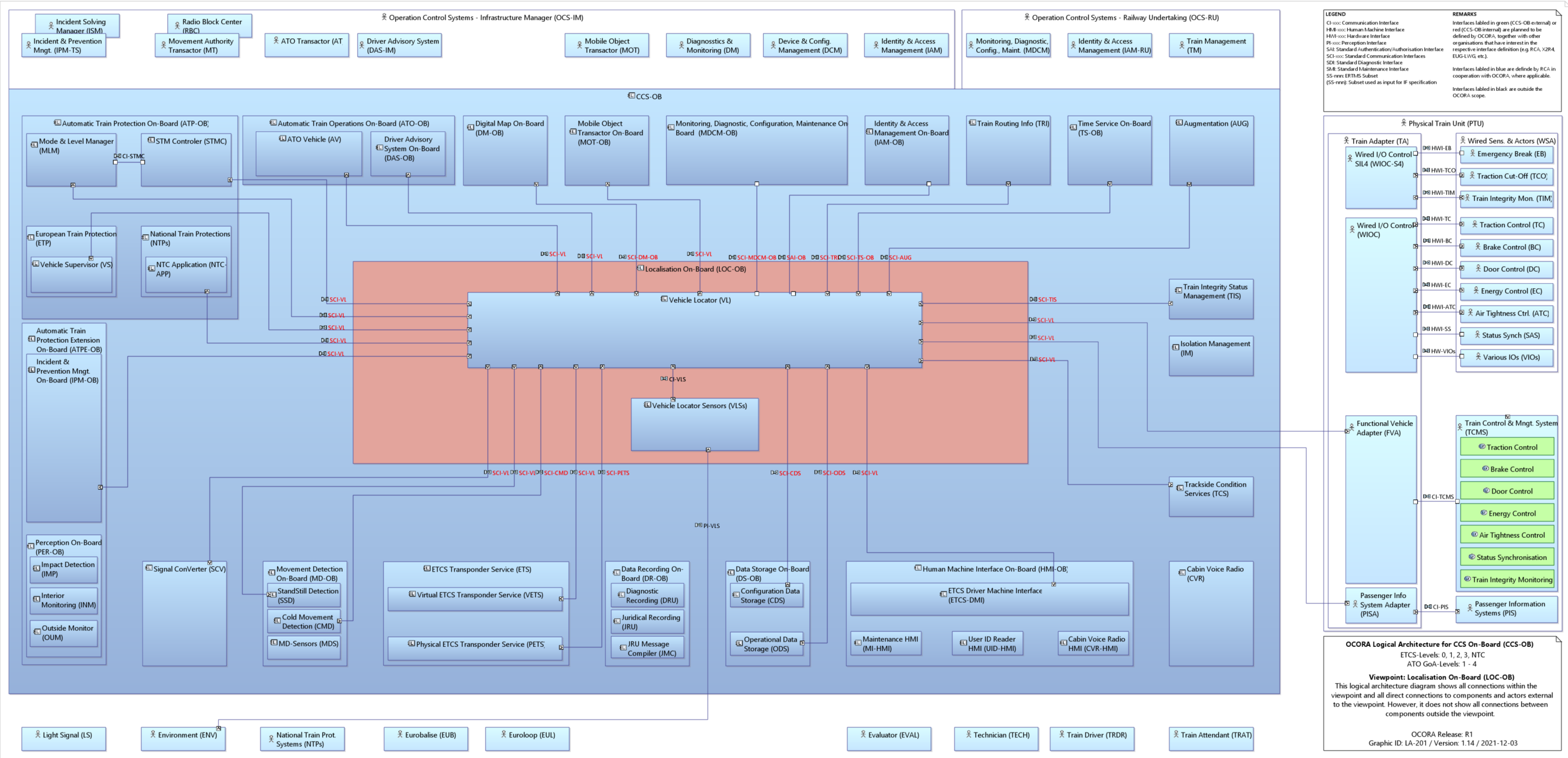

Figure 41 CCS-OB logical architecture – Viewpoint LOC-OB