OCORA

Open CCS On-board Reference Architecture

System Architecture
Gamma Release

This OCORA work is licensed under the dual licensing Terms EUPL 1.2 (Commission Implementing Decision (EU) 2017/863 of 18 May 2017) and the terms and condition of the Attributions- ShareAlike 3.0 Unported license or its national version (in particular CC-BY-SA 3.0 DE).

Document ID: OCORA-40-001-Gamma

Version: 1.02

Date: 04.12.2020

Status: Final

Revision history

Version	Change Description	Initial	Date of change
0.00	▪ Beta Release - Version 1.01 as starting point	AL	2020-07-01
1.00	▪ Various updates for OCORA Gamma Release	ML AL CG TM	2020-11-18
1.01	▪ Review feedback received until 2020-11-26 considered	AL	2020-12-07
1.02	▪ Review feedback received until 2020-12-01 considered ▪ Open issue resolved during release conference	AL ML	2020-12-04

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.

The following references are used in this document:

[1] OCORA-10-001-Gamma – Release Notes

[2] OCORA-10-003-Gamma – Feedback Form

[3] OCORA-20-003-Gamma – Technical Slide Deck

[4] OCORA-20-005-Gamma – Technical Posters

[5] OCORA-30-001-Gamma – Introduction to OCORA

[6] OCORA-30-002-Gamma – Problem Statements

[7] OCORA-30-006-Gamma – High Level Methodology

[8] OCORA-30-009-Gamma – Requirements

[9] OCORA-40-003-Gamma – UVCC Bus Evaluation

[10] OCORA-40-004-Gamma – Computing Platform - Whitepaper

[11] OCORA-40-005-Gamma – Functional Vehicle Adapter – Introduction and Overview

[12] OCORA-40-006-Gamma – CCS-TCMS Interface – ETCS Functionality (SS119)

[13] OCORA-40-007-Gamma – CCS-TCMS Interface – ATO Functionality (SS139)

[14] OCORA-40-009-Gamma – (Cyber) Security – Overview

[15] OCORA-40-013-Gamma – Computing-Platform-Requirements

[16] OCORA-90-001-Gamma – Question and Answers

[17] OCORA-90-002-Gamma – Glossary

[18] RCA.Doc. 2, Beta.1, RCA Architecture Overview

[19] ERA_ERTMS_015560

[20] ERTMS User Group Document 97E2675B

Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). We always reference to the latest available official version of the SUBSET, unless indicated differently.

1 Introduction

1.1 Document context and purpose

This document is published as part of the OCORA Gamma release, together with the documents listed in the release notes [1]. It is the third release of this document which will be further developed in consecutive releases.

The document is provided in PDF format with searchable text and hyperlinks. The links are not only available for the directory, the table of figures, and the table of tables, but also for references to interface descriptions (green and red boxes) and all references to chapters and referenced documents. The latter are highlighted in blue to indicate the hyperlink functionality. Upon request, this document and all its graphics can be made available in the native data format (e.g. Word, PowerPoint, Visio).

Subsequent releases of this document (Delta, etc.) and topic specific documentation will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

This 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 aims to provide the reader:

- the system concept (chapter 2.1.2), containing information typically used for CENELEC phase 1 (refer to definitions in document [7]). This includes a clear definition of the scope, purpose, and content of the OCORA architecture.
- an identification and abstract description of all components (hardware & software) and building blocks.
- an introduction to digitalisation-specific topics, such as the cyber security, etc.
- proposition on various topics, such as the OCORA gateway, the connectivity with data centres, diagnostics, and maintenance, etc.

From all the topics discussed in this OCORA Gamma release, the identification of three protocol variants for the OSI layer 5 (refer to OCORA OSI definitions in document [7]) for the universal vital command and control bus (UVCCB) is considered to be the most important message. A description of the evaluated bus technologies and the respective considerations can be found in document [20]. Furthermore, the explanation for different variants of the CCS On-Board / UVCCB integration into the train networks is described.

The Computing Platform - Whitepaper [10], the Functional Vehicle Adapter – Introduction and Overview [11], the CCS-TCMS Interface [12], [13], and the (Cyber) Security – Overview [14] provide further details of the OCORA architecture.

1.2 Why should I read this document and how to provide feedback?

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA technical concepts for on-board CCS. The reader will gain insights regarding the topics listed in chapter 1.1, and 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 gamma release documentation can be given by using the feedback form [2].

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

If you are an organization interested in developing CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development. Subsequent version of this document aims to provide information needed for CENELEC phase 2 – 5 (refer to OCORA CENELEC interpretation in document [7]).

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 this specification document, we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Question and Answers [16] and the Glossary [17].

Selected graphics provided in this document are available, in a larger scale, in the documents [3] and [4], and in Appendix G.

2 System concept

2.1 System under consideration

2.1.1 Scope

OCORA aims at providing the architecture for a CCS on-board solution that is compliant with trains equipped with a NG-TCN (Next/New Generation – Train Control Network) while also supporting legacy trains. For defining the system under consideration (scope, context, etc.), we are using the legacy train scenario. Refer to Appendix B for the different scenarios considered at this point in time.

To identify the scope, OCORA has developed a hardware block diagram (Figure 1) and a functional block diagram (Figure 2). Both diagrams identify the CCS On-Board and the OCORA Core scope while also depicting the respective context (actors and external systems). A brief description of the actors and external systems can be found in chapter 2.1.3.

The system under consideration of the OCORA program is the “CCS On-Board” (green box) as identified in Figure 1 from a hardware point of view and in Figure 2 from a functional perspective. 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 [7]).

From an OCORA system architecture and design perspective, the focus is on the “OCORA Core” (red box) as depicted in Figure 1 and in Figure 2. For the “Peripheral Devices” and the “Connectivity Devices” (outside the red box), OCORA will only provide interface specifications, high-level functional requirements, and non-functional requirements. These are all requirements and specifications needed to ensure “plug & play”-like exchangeability. Of course, these specifications are only developed by OCORA for the components not already sufficiently standardised and where no standard is being developed by other organizations.

To summarize: “Peripheral Devices” and “Connectivity Devices” are external systems in relation to the OCORA Core architecture, hence only interface specifications, high-level functional and non-functional requirements will be provided. From a RAMSS point of view, they are CCS On-Board components, and hence in scope for RAMSS analysis.

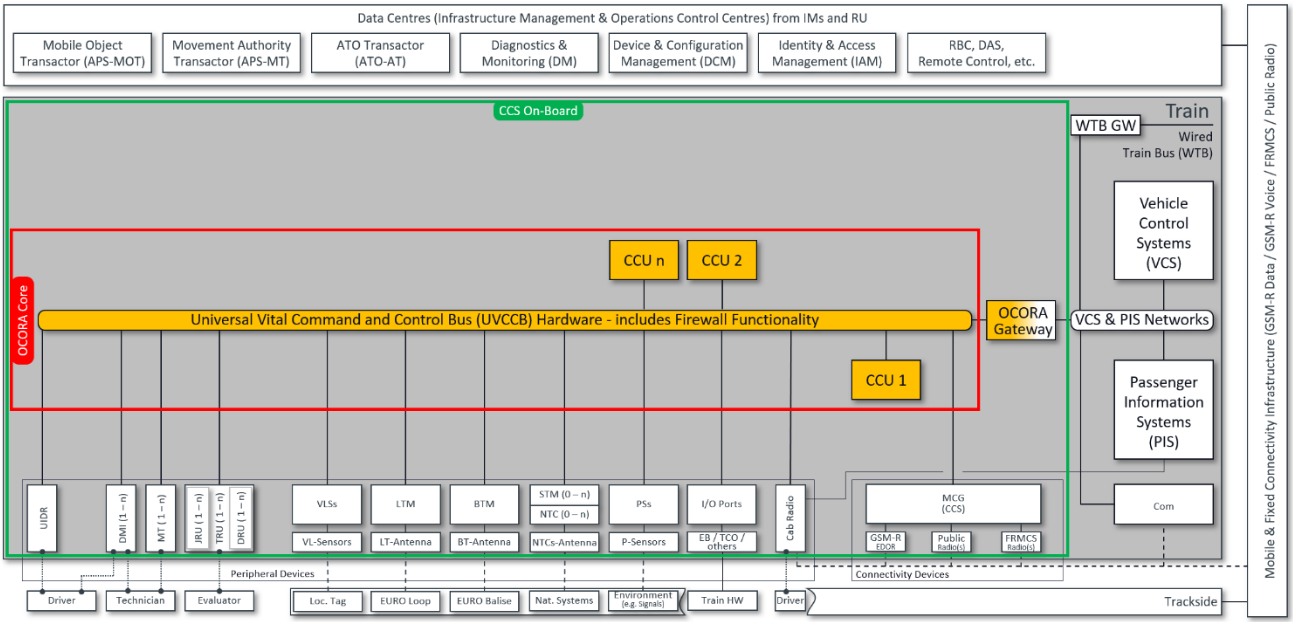

Figure 1 Scope – hardware view
(refer to Appendix G1 for large scale representation)

Remarks to Figure 1 and in Figure 2: solid lines indicate wired connections, dotted lines represent user interactions, and dashed lines “over the air” communication. Large scale graphics of Figure 1 and in Figure 2 can be found in Appendix G1.

To define the architecture, OCORA has identified components for the “CCS On-Board” (blocks inside the green box).

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

Every component can consist of sub-components. Currently, the OCORA architecture focuses just on the component and not on the sub-component level. Further decomposition will be addressed in subsequent releases. All components are described in more detail in chapter 4.

As explained in document [5], 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 to n component(s). It is the OCORA vision to provide “plug & play”-like exchangeability for all building blocks and not for all CCS On-Board components as identified in Figure 1 and in Figure 2. Refer to chapter 3 for the currently proposed OCORA building blocks.

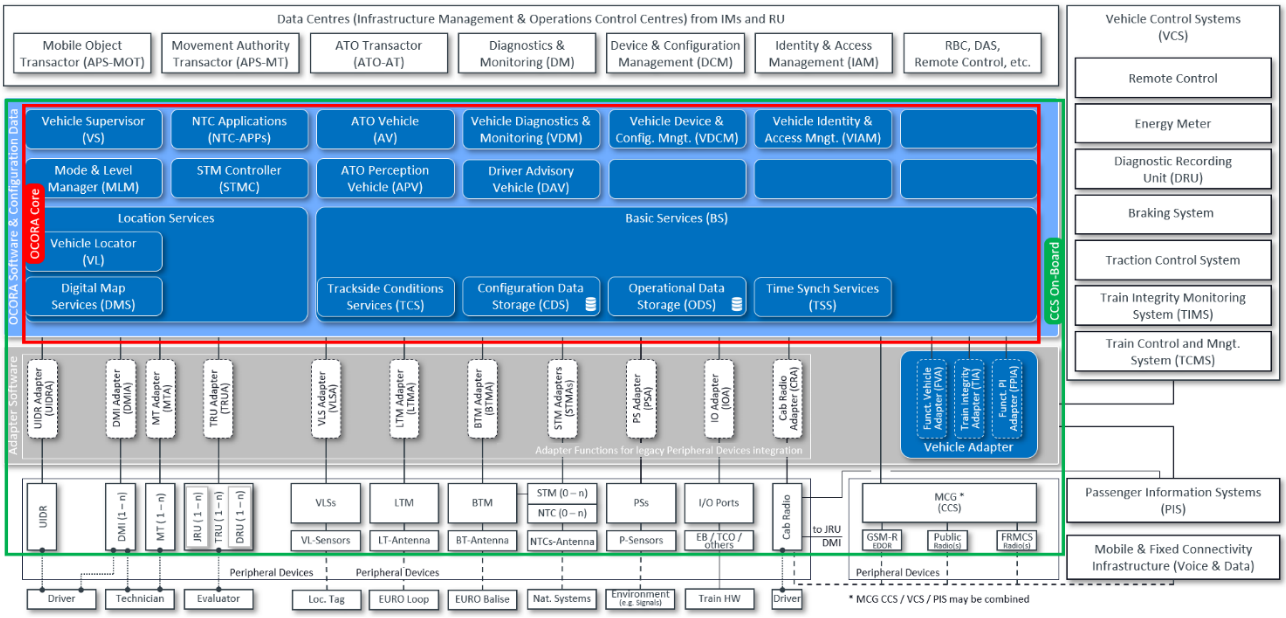

Figure 2 Scope – functional view
(refer to Appendix G2 for large scale representation)

The components within the “CCS On-Board” as identified in Figure 1 and in Figure 2 support ETCS L1 – L3, level National Train Controls (NTCs), ATO GoA1 – GoA4 over ETCS and/or over NTC, and the potential to resolve error corrections and NNTRs (Notified National Technical Rules). The “empty boxes” in Figure 2 indicates that the architecture is open to implement functionality, not envisioned at this point in time. The UVCCB and the modular architecture provide the base for enabling this.

The configuration for a specific implementation is open and may include only a subset of the components represented in Figure 1 and in Figure 2. But not only the number of deployed components can differ between implementations. The functionality of some of the hardware components (Figure 1) 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 on-board 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 7 and document [10] for details on the computing platform, that supports the separation of hardware from software.

The components / building blocks identified in Figure 1 and in Figure 2 represent just a high-level view, abstracting many details. For example: The UVCCB, 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 C).

Last but not least, the representation in Figure 1 and Figure 2 show, as already mentioned, one possible deployment scenario (scenario 1a); especially regarding the OCORA Gateway (OCORA-GW) and how the connectivity devices (GSM-R Radio, Public Radio, FRMCS Radio) and the train networks (VCS, PIN) are connected. For this aspect alone, many deployment scenarios exist that need further investigations. Refer to Appendix C for a discussion of the different scenarios. Depending on the specific situation, one or the other scenario may be preferred. Nevertheless, OCORA aims to reduce the proposed scenarios to the most relevant ones. The connection between Passenger Information Systems and OCORA Core is, for instance, dependent on security requirements of the vehicle. It will be clarified in future releases of this documentation.

All identified components, and external systems are described further in subsequent chapters of this document. Chapter 2.1.1.1 provides a list and a short description of all hardware components, including references to more detailed information and chapter 2.1.1.2 provides the same for functional/software components.

To define the scope boundary to the necessary detail, all envisioned interfaces are identified from a hardware point of view and on a functional level. Equally, for the “CCS On-Board” scope (refer to chapter 5) and the “OCORA Core” scope (refer to chapter 6).

2.1.1.1 Hardware components

Figure 1 on page 11 and Appendix G1 depict the currently identified hardware components, in scope of CCS on-board. A high-level description including links to more detailed information for each of the hardware components is provided in the subsequent tables of this chapter.

OCORA core hardware

The OCORA core hardware are the components within the "OCORA Core" scope. For these components, OCORA not provides interface specifications, high-level functional requirements, and non-functional requirements. The OCORA core hardware is also considered for all RAMSS aspects.

The OCORA core hardware, together with the runtime environment (refer to chapter 7), provides the platform to run the OCORA core functionality.

OCORA Core Hardware		
Component	**High-Level Description**	**Link to Further Information**
UVCCB	**Universal Vital Control and Command Bus** The Universal Vital Command and Control Bus (UVCCB) is the CCS on-board bus/network allowing direct communication between all CCS on-board components connected to it and eventually with external systems, such as the TCMS. The UVCCB 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 UVCCB is a TSN Ethernet based network with the use of SDTv2/v4 as safety layer. The bus/network is currently defined for OSI layer 1 to 2 and to a certain extent for OSI layer 3 to 5 (refer to OCORA OSI definitions in document [7]). At the final stage the UVCCB will be specified up to OSI layer 6 and 7 (refer to OCORA OSI definitions in document [7]) in subsequent versions of the OCORA specifications. Refer to Appendix C for a detailed discussion on the network topology scenarios that OCORA considers for implementing the UVCCB.	▪ Chapter 4.1.1 ▪ Appendix C ▪ Document [9]
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 7 for details).	▪ Chapter 4.1.2 ▪ Chapter 7 ▪ Document [10]
OCORA-GW	**OCORA Gateway** The OCORA Gateway (OCORA-GW) is a piece of hardware providing communication capabilities between the UVCCB (CCS-ECN) 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 [7]). 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 VCS/PIS networks are using the same technology, The OCORA-GW is not needed, and an ECN/ECN Gateway ensures security and performance.	▪ Chapter 4.1.3

Table 1 OCORA core hardware

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 pro - cess for drivers and service technicians. RFID card readers may be the most com- mon 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 4.2.1
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 Voice, etc.). In such configurations, the additional DMI may also be used to increase availability of the primary display functions through a switch-over mechanism. Mo- bile personal devices (e.g. Tablets) are another type of DMI that may be used for some applications.	▪ Chapter 4.2.2
MT (1 – n)	**Maintenance Terminal** The Maintenance Terminal (MT) is a laptop that can be connected to the UVCCB 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 4.2.3
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 4.2.4
VLSs	**Vehicle Localisation Systems** The Vehicle Localisation Systems (VLSs) processes the data from the various Vehicle Localisation Sensors, performs the necessary sensor fusion, and provides the data to the VL through the UVCCB.	▪ Chapter 4.2.5
VL-Sensors	**Vehicle Localisation Sensors** The Vehicle Localisation Sensors (VL Sensors) provide raw data to determine speed, direction of travel, acceleration, position, and cold movement information to the Vehicle Localisation System (VLS). Depending on the RU's need and the pro- gress of technology (e.g. GNSS, IMU) different type and quality of sensors may be used.	▪ Chapter 4.2.6
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 UVCCB.	▪ Chapter 4.2.7

Peripheral Devices		
Component	**High-Level Description**	**Link to Further Information**
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 4.2.8
BTM	**Balise Transmission Module** 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 UVCCB, for the ETCS application (VS). Optionally, the BTM can also receive data from KER Balises and can make the data available, through the UVCCB, to the corresponding STM through the K interface describe in SUBSET-101.	▪ Chapter 4.2.9
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 can provide the data to the Balise Transmission Module (BTM).	▪ Chapter 4.2.10
STM	**Specific Transmission Module** The Specific Transmission Module (STM) provides the connection between the ETCS system (in case of OCORA the UVCCB) 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 4.2.11
NTC	**National Train Control** The National Train Control (NTC) provides Automated Train Protection functionality on national level. It communicates with other OCORA components, namely the STM Controller (STMC) and can also use the functionality of other components connected to the UVCCB (e.g. DMI, VLS, TCO, EB, etc.). Alternatively, it is also possible to implement the National Train Controls business logic as Applications on the OCORA computing platform (see NTC-APPs for more information). In this case, the NTC-APPs access through the UVCCB and the BTM the balise data in order to get the packet 44 information.	▪ Chapter 4.2.12
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 4.2.13
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 UVCCB.	▪ Chapter 4.2.14
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, but can also include vibration sensors, smoke detectors, etc.	▪ Chapter 4.2.15
I/O Ports	**Input/Output Ports** The I/O Ports provide access between the UVCCB and certain actuators and sensors. The status of the sensors is processed by this component and made available on the UVCCB and commands from the various CCS on-board components, sent through the UVCCB, are applied to the respective port.	▪ Chapter 4.2.16

Peripheral Devices		
Component	**High-Level Description**	**Link to Further Information**
EB / TCO / Others	**Emergency Brakes / Traction Cut-Off / Others** These are the devices triggering the Emergency Brake (EB) and the Traction Cut-Off (TCO) for ETCS, NTC-APP, APV, etc. Depending on the system configuration and RU's need, multiple EBs and TCOs can be connected and additional I/Os can be used to interact with "other" external systems, actuators, and sensors. Examples are: ▪ Cabin activation status ▪ ETCS isolation status ▪ Vehicle power status ▪ Dead Man Switch: to monitor the awareness of the driver ▪ CCS Cabinet Supervision: to monitor unauthorized access	▪ Chapter 4.2.17
Cab Radio	**Cabin Radio** The Cabin Radio 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 HMI, 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 Cab Radio 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 between the CCS data and cabin voice. The OCORA concept foresees providing voice communication through voice over IP (VoIP) and to connect to the PIS, DMI and the JRU through the UVCCB.	▪ Chapter 4.2.18

Table 2 Peripheral devices

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 C for a discussion of possible options.

Connectivity Devices		
Component	**High-Level Description**	**Link to Further Information**
MCG (CCS)	**Mobile Communication Gateway (CCS)** The Mobile Communication Gateway (MCG (CCS)) provides train to track-side communication for the on-board CCS and depending on the vehicle, it may also provide track-side connectivity for the systems of the Train Control bus (VCS and PIS). The GSM-R and the FRMCS Radio will be either part of the MCG (CCS) or will be connected to the MCG (CCS), providing 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.	▪ Chapter 4.3.1
GSM-R – EDOR Radio	**Global System for Mobile Communications Railway – 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 eventually be replaced by an FRMCS Radio.	▪ Chapter 4.3.1
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, 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 4.3.3
FRMCS Radio (1 – n)	**Future Rail Mobile Communication System 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 4.3.4

Table 3 Connectivity devices

2.1.1.2 Software components

Figure 2 on page 11 and Appendix G2 on page 97 depict the currently identified software components, in scope of CCS on-board. A high-level description including links to more detailed information for each of the software component is provided in the subsequent tables of this chapter.

OCORA software and configuration data

The OCORA software and configuration data provides the actual (business) logic and configuration data for the CCS on-board functions and functionality to be able perform maintenance tasks efficiently. At the current stage, a set of software components are identified. However, more software components will be defined in subsequent versions of this document. But the OCORA platform also provides an API that allows new software components, not known at this point in time, to use the services of the platform and the infrastructure of the vehicle. Hence, developing and deploying new functionality should be simplified. Such software components could be “automated routine test” or an NTC application that uses balise data, packet 44.

All OCORA software components run on the OCORA computing platform (refer to chapter 7).

OCORA Software and Configuration Data		
Component	**High-Level Description**	**Link to Further Information**
VS	**Vehicle Supervisor** 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 4.4.1
MLM	**Mode & Level Manager** 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 4.4.2
NTC-APPs	**National Train Control Applications** The National Train Controls Applications (NTC-APPs), deployed on the OCORA computing platform, are safe applications in charge of ensuring automated train protection based on national systems. NTC-APPs, implemented on the OCORA computing platform, must communicate, as a minimum, with the ATP Manager 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 TRU, DMI can be used, the TCMS can be accessed through the Functional Vehicle Adapter (FVA), etc.	▪ Chapter 4.4.3
STMC	**STM Controller** 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 automated transition from ETCS to the national ATP system and vice versa while the vehicle is driving.	▪ Chapter 4.4.4

OCORA Software and Configuration Data		
Component	**High-Level Description**	**Link to Further Information**
AV	**ATO Vehicle** The ATO Vehicle (AV) application, deployed on the OCORA computing platform, is a non-safe application for automated train operations. A safe extension is needed for GoA3 and GoA4 operations. This is provided by the ATO Perception Vehicle (APV). 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 4.4.5
APV	**ATO Perception Vehicle** The ATO Perception Vehicle (APV) application, deployed on the OCORA computing platform, is a safe application needed for automated train operations with GoA3 and GoA4. In case of light signalling perception, the APV may also be used in GoA2. It is deployed in addition to ATO Vehicle (AV) and includes all safety-related functionality and data needed for GoA3 and GoA4 operations. To execute these tasks, it has interfaces to perception system, Digital Maps (DMS), etc. Based on the situation (type of danger and location information) it triggers speed reduction, service brakes, traction cut-off, pantograph drop, horn, and emergency brakes. Remark: APV is called "Incident Protection Management" (IPM) in GoA3 – GoA4 Shift2Rail discussions. There is an open possibly that APV may be indirectly linked – through a Signalling ConVerter (SCV) - to the VS in order to emulate lateral signalling into ETCS messages.	▪ Chapter 4.4.6
DAV	**Driver Advisory Vehicle** The Driver Advisory Vehicle (DAV) application 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) or the Traffic Management System (TMS) is responsible for conflict detection and calculation of new target train timings, that are forwarded to the DAV and evaluated accordingly. The typical integration of DAV application is defined EN 15380-4. The DAV can also operate standalone (e.g. without integration into the vehicle). The DAV is not needed if ATO Vehicle (AV) is installed, since the AV already includes the DAV functionality. The implementation of DAV application on OCORA computing platform is an open issue to be solved in subsequent versions of this document (unsafe information displayed on the driver DMI).	▪ Chapter 4.4.7
VDM	**Vehicle Diagnostics & Monitoring** The Vehicle Diagnostics & Monitoring (VDM) service, 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 standardized format. For remote diagnostics and monitoring the data can be send 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). While the TRUA provides the data for recording in the TRU, the VDM provides the data to other systems such as the centralized DMs or the Maintenance Terminals.	▪ Chapter 4.4.8
VDCM	**Vehicle Device & Configuration Management** The Vehicle Device & Configuration Management (VDCM) service, deployed on the OCORA computing platform, allows for local (through the Maintenance Terminal) and remote (through the centralized 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).	▪ Chapter 4.4.9

OCORA Software and Configuration Data		
Component	**High-Level Description**	**Link to Further Information**
VIAM	**Vehicle Identity & Access Management** The Vehicle Identity & Access Management (VIAM) 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 application 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 UVCCB 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 unauthorized access to resources and functions within the CCS on-board system.	▪ Chapter 4.4.10
Location Services		
VL	**Vehicle Locator** The Vehicle Locator (VL) is a safe service deployed on the OCORA computing platform. It provides the actual position/direction in relation to infrastructure elements to the VS, where the actual position/direction and the current speed are aggregated with other data into a Train Position Report (TPR). Localisation data may be sent by the VL to APS-MOT, containing e.g. ETCS irrelevant data (not used by VS). The VL sends the full virtual track occupation of the train or only a part of it (only the front or rear position). The VL can use different localization technologies, from today’s “balise + odometry” to additional sensor inputs such as GNSS or inertial measurement units. To access the respective sensors, the VL interacts with the Vehicle Localisation Systems (VLSs).	▪ Chapter 4.4.11.1
DMS	**Digital Map Services** The Digital Map Service (DMS) is a safe service deployed on the OCORA computing platform. The DMS 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, APV) 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 DMS uses its own on-board data storage that is updated, if required, using the functionality of the Vehicle Device & Configuration Management (VDCM) to propagate trackside map data (e.g. from Topo4) to the on-board data storage.	▪ Chapter 4.4.11.2
Basic Services		
TCS	**Trackside Condition Services** 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 through IF490 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.	▪ Chapter 4.4.12.1
CDS	**Configuration Data Storage** 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. VDM). 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 Vehicle Device & Configuration Management (VDCM) component. In subsequent versions of the OCORA specifications, the CDS will be specified in detail.	▪ Chapter 4.4.12.2

OCORA Software and Configuration Data		
Component	**High-Level Description**	**Link to Further Information**
ODS	**Operational Data Storage** 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, etc. In subsequent versions of the OCORA specifications, the ODS will be specified in detail.	▪ Chapter 4.4.12.1
TSS	**Time Synchronisation Service** The Time Synchronisation Service (TSS) provides a service that allows all on-board components to have their time in synch with each other and synched with the trackside systems (e.g. safe data centres). The time base is UTC and components in need to display the time can revert it to local time. This functionality is significant to simplify diagnostic and analysis, for ATO operations, and other aspects.	▪ Chapter 4.4.12.4

Table 4 CCS on-board components – OCORA Software & Configuration Data

Adapter software

The adapter software contains software components that allow abstracting the different type of train hardware towards the standard OCORA software. The goal of these software components is to ensure that the interfaces with the OCORA software remain the same, regardless of the underlying train hardware.

The adapter software components run on the peripheral devices, or on a specific adapter hardware, or, in some cases, on the OCORA Gateway.

The adapters software for adapting legacy peripheral devices are outside of the OCORA scope and are therefore not considered any further by OCORA. It is the device vendor's responsibility to adapt to the OCORA standard. However, the adapters towards the VCS and PIS are within the scope of the OCORA program and therefore further detailed below.

Adapter Software		
Component	**High-Level Description**	**Link to Further Information**
FVA	**Functional Vehicle Adapter** The Functional Vehicle Adapter (FVA) is a piece of software deployed on the OCORA computing platform, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardized interface towards the CCS applications and services for vehicle functions and vehicle information needed by the OCORA on-board applications and services. Although the TSI-CCS SUBSET-034, SUBSET-119, and SUBSET-139 are defining the interface to the TCMS system, vehicle 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. In addition, the FVA can also be used to integrate vehicles through wired connections. Also, the standardized interface to the CCS applications evolves in multiple iterations as outlined in chapter 3. 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 other context a piece of hardware is meant. To avoid confusion, OCORA does not use the term TIU.	▪ Chapter 4.5.1 ▪ Document [11], [12], [13]
TIA	**Train Integrity Adapter** The Train Integrity Adapter (TIA) is a safe piece of software 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 service 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 standardized interface, independent of the option used. The train integrity status may also include the total safe train length (including the length over coupled compositions).	▪ Chapter 4.5.2
FPIA	**Functional Passenger Information Systems Adapter** The Functional Passenger Information Adapter (FPIA) 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 standardized interface towards the Passenger Information System (PIS), allowing the PIS to receive CCS of interest to the PIS.	▪ Chapter 4.5.3

Table 5 CCS on-board components – Adapter Software

2.1.2 Context

Information about the context in which the OCORA architecture is being developed, can be found in document [5], and [6]. The technical context is described in chapter 2.1.3.

2.1.3 Environment

The environment consists of all actors and systems that interact with the CCS On-Board system and the environment conditions in which the CCS on-board system operates.

2.1.3.1 Actors

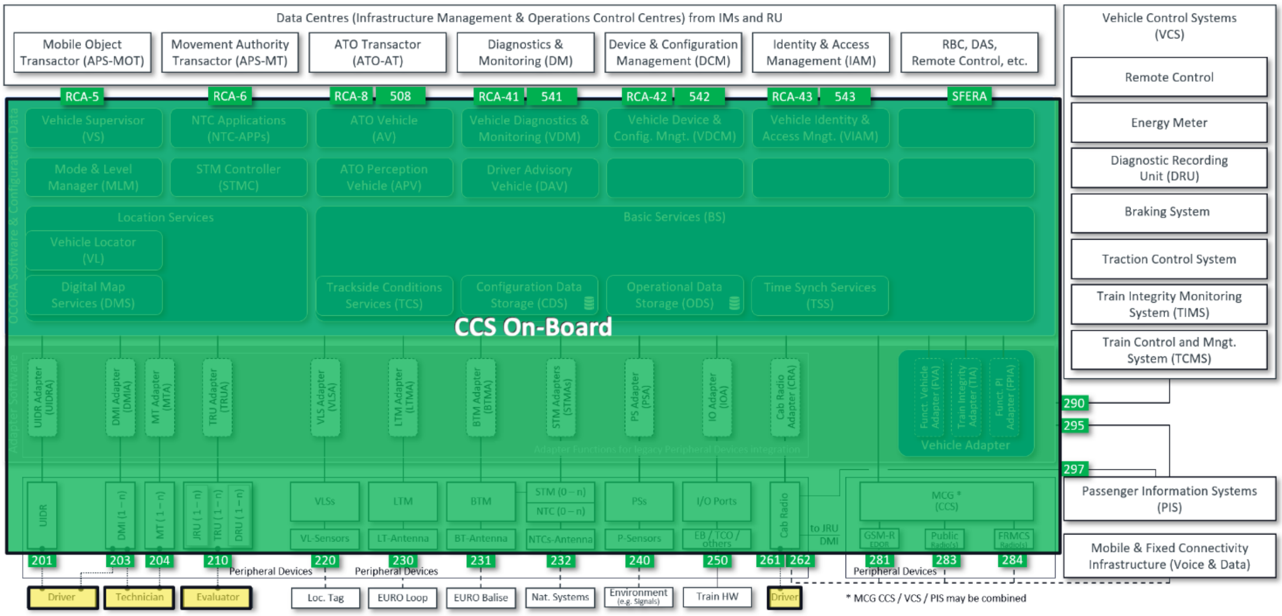

Figure 3 CCS On-Board Actors (yellow boxes)

The actors are the users of the CCS on-board system. The actors currently identified, including their roles, are listed in the following table.

Actor	Role
Driver	The person who operates the vehicle and may hold a user identification card. Refer also to interfaces: 201 203 261
Technician	The person who performs preventive and corrective maintenance tasks. Refer also to interfaces: 203 204
Evaluator	The person evaluating data stored in the TRU. Refer also to interfaces: 210

Table 6 Actors and roles

In subsequent versions of this document, OCORA aims at synchronizing the actors and their roles with definitions used in other programs, such as RCA and X2RAIL.

2.1.3.2 External systems

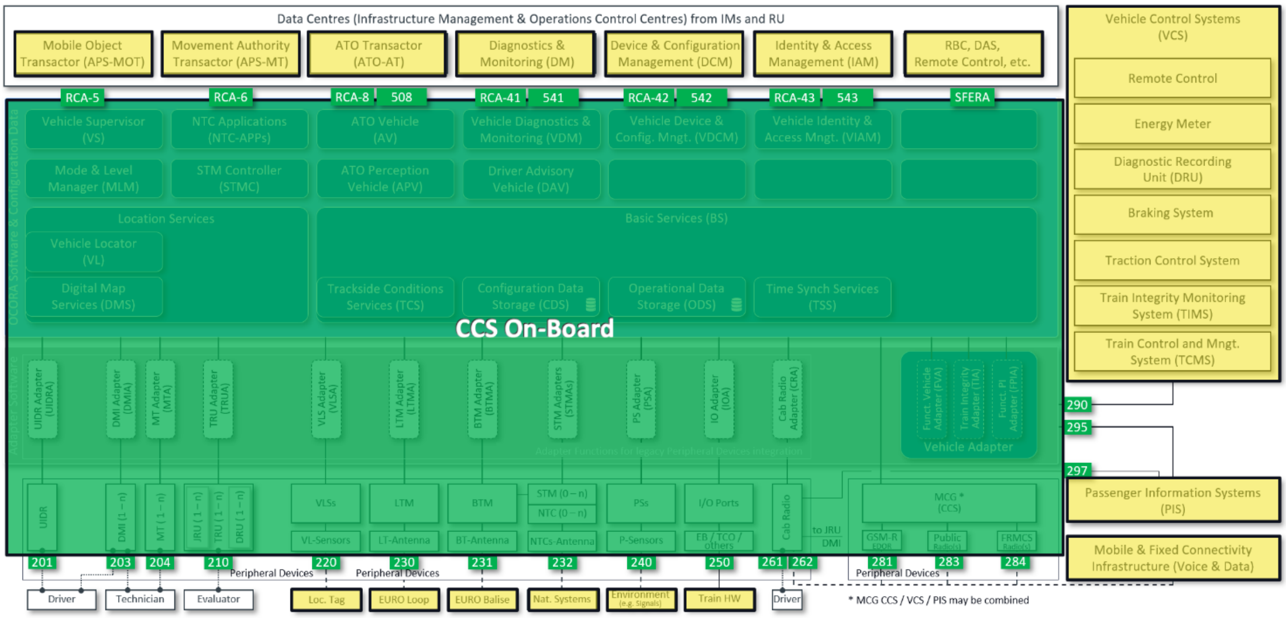

Figure 4 CCS On-Board External Systems (yellow boxes)

External systems are all systems that interact with the CCS on-board system. This includes the track side equipment, the mobile & fixed connectivity infrastructure, and the data centres form the IMs and the RU. The external systems currently identified, including a brief description and link to the interface description are listed in the Table 7.

In addition to the external systems described in Table 7, there are also mechanical systems (e.g. cabinets) and electrical systems (e.g. UPSs) interacting with the CCS on-board system. These systems will be considered in more detail in subsequent versions of the OCORA documentation.

External System	High-Level Description	Link to Interface Description
Trackside Equipment		
Loc. Tag	**Location Tag** The location tags can be any kind of tag installed on trackside infra-structure elements, providing the Vehicle Localisation System the ability to determine the absolute position of the vehicle. These tags can be bar codes, RFID tags, etc.	220
EURO Loop	**EURO Loop** A transponder loop mounted along the track, which can communi-cate with a train passing along, compliant to the ERTMS/ETCS spe-cifications.	230
EURO Balise	**EURO Balise** A transponder, mounted on the track, which can communicate with a train passing over it, compliant to the ERTMS/ETCS specifications.	231
National Systems	Any kind of national Automated Train Protection (ATP) system.	232
Environment	Any kind of signals, obstacles, etc.	240
Train Hardware	Any kind of train hardware such as EB and TOC access	240
Mobile & Fixed Connectivity Infrastructure		
This includes all communication infrastructure needed by the vehicle.		262 281 283 284
Train / Vehicle		
Train Control Systems	Any kind of Train Control Network/Bus/Cables and its connected systems.	290

External System	High-Level Description	Link to Interface Description
Passenger Information Systems	Any kind of Passenger Information Network and its connected systems. This does not include the network for passenger internet services.	295
Passenger Information Systems	UIC connection between the Cab Radio and the Passenger Information Systems.	297
Data Centres (Infrastructure Management & Operations Control Centres) from IMs and RU		
APS-MOT	**Advanced Protection System - Mobile Object Transactor** RCA definition as per document [18]: 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.	RCA-5
APS-MT	**Advanced Protection System - Movement Authority Transactor** RCA definition as per document [18]: 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.	RCA-6
ATO-AT	**ATO Transactor** RCA definition as per document [18]: ATO-AT implements the communication with all registered ATO vehicles and provides the standardized interface.	RCA-8
ATO-AT (from RU)	**ATO Transactor from RU** This is only needed for GoA L3–4 (when no driver is present) for driving trains outside the timetable (e.g. to the depot).	508
DM	**Diagnostics & Monitoring** RCA definition as per document [18]: 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 IM, which triggers the corrective maintenance actions. It must be noted that there is the need for a DM system operated by the IM 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.	RCA-41 541
DCM	**Device & Configuration Management** RCA definition as per document [18]: 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 IMs 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.	RCA-42 542
IAM	**Identity & Access Management** RCA definition as per document [18]: 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 IM 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.	RCA-43 543

External System	High-Level Description	Link to Interface Description
DAS	**Driver Advisory System** The Driver Advisory System (DAS) application, is a non-safe application. It generates, together with the Driver Advisory Vehicle (DAV) application, detailed driver advice for adhering to the planned timings while driving energy efficient. The DAS is responsible for conflict detection and calculation of new target train timings, that are forwarded to the Driver Advisory Vehicle (DAV) application. The DAV is responsible to calculating an energy efficient speed profile to achieve the pre-planned and dynamically updated train timings. The DAS communicates with the DAV, using the SFERA specification.	SFERA
RBC	**Radio Block Centre** [1] 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.	SUBSET-026

Table 7 External systems

In subsequent versions of this document, OCORA aims at synchronizing the naming and description of the external systems with definitions used in other programs, such as RCA and X2RAIL.

[1] https://en.wikipedia.org/wiki/European_Train_Control_System

2.1.3.3 Environmental conditions

The environment conditions, in which the different components of the CCS on-board system operate, depend on the location the component is installed. The possible installation locations are defined in EN 50155: 2017, appendix C. Figure 5 depicts the foreseen installation locations and Table 8 provides explanations regarding these locations.

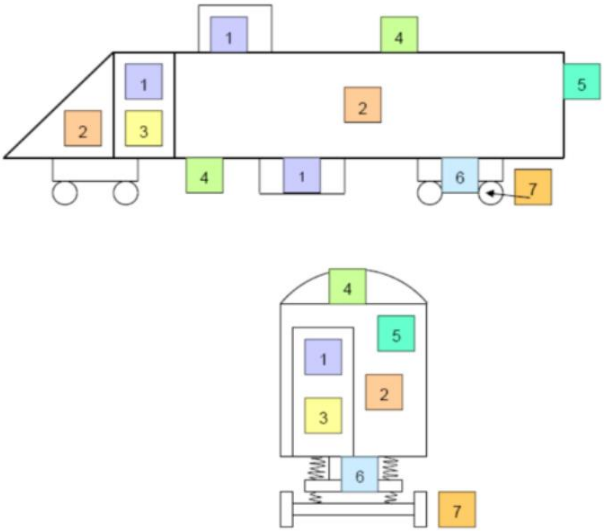

Figure 5 Typical location positions for on-board rolling stock (EN 50155: 2017)

Location ID (see Figure 5)	Definition	Examples	Examples of consequences on requirements
1	closed electrical operating area	▪ interior vehicle cubicle (weather-protected) ▪ exterior vehicle cubicle (weather-protected) ▪ either under-frame or upper-roof	▪ Operating temperatures and/or shock levels ▪ depending on the location of the installation.
2	cabin and interiors	▪ passenger vehicle compartment ▪ driver cabin	▪ low IP code required (air with low dust and chemical contamination
3	closed electrical operating area; forced filtered ventilation with outside air	▪ machinery compartment	▪ higher operating temperature in case of engine/power converter compartment or ▪ resistance to fuels and fluids
4	outdoor static applications	▪ under car body, roof (non-weather protected)	▪ non weather-protected location higher IP code ▪ resistance to light (UV) ▪ resistance to ozone for rubber and plastic parts
5	outdoor dynamic applications	▪ inter-vehicle	▪ non weather-protected location higher IP degree ▪ resistance to light (UV) ▪ resistance to ozone for rubber and plastic parts ▪ higher mechanical resistance
6	outdoor highly dynamic applications	▪ bogie	▪ non weather-protected location higher IP code ▪ resistance to light (UV) ▪ resistance to ozone for rubber and plastic parts ▪ higher mechanical resistance ▪ high vibration and shock constraints ▪ resistance to fuel and fluids
7	outdoor highly dynamic applications	▪ axles	▪ non weather-protected location higher IP code ▪ resistance to light (UV) ▪ resistance to ozone for rubber and plastic parts ▪ higher mechanical resistance ▪ very high vibration and shock constraints ▪ resistance to fuels and fluids

Table 8 Explanation of typical location positions for on-board rolling stock (EN 50155: 2017)

The definitions of the environmental conditions applicable for OCORA components will be provided in a subsequent version of the OCORA documentation.

2.1.4 Purpose

The purpose of the OCORA program is to:

provide an open and modular CCS on-board reference architecture, allowing for “plug & play”-like exchangeability of the defined pre-certified building blocks, supporting maximum independency, and the acceptance of global standards.

Refer to document [5], and [6], for details about the motivation that drives this purpose and to [8] for OCORA objectives.

The technical purpose of the CCS on-board system is to:

- prevent accidents such as collision between trains, derailment due to overspeed, damage by reason of indication negligence, etc.
- allow for Automated Train Operations (ATO) at all Grades of Autonomy levels (GoA 1 - 4) and in combination with different Automated Train Protection (ATP) systems (ETCS and/or NTC).

Refer to chapter 2.1.1 for details about the scope.

2.2 RAMSS performance and requirements of similar and/or previous systems

This chapter will be provided as part of a subsequent release of this documentation.

2.3 RAMSS performance and requirements for CCS on-board system

2.3.1 Reliability

This chapter will be provided as part of a subsequent release of this documentation.

2.3.2 Availability

This chapter will be provided as part of a subsequent release of this documentation.

2.3.3 Maintainability

This chapter will be provided as part of a subsequent release of this documentation.

2.3.4 Safety

This chapter will be provided as part of a subsequent release of this documentation.

2.3.5 Security

Refer to chapter 8.

2.4 RAMSS policies and targets from railway undertakings

This chapter will be provided as part of a subsequent release of this documentation.

2.5 Safety legislation

This chapter will be provided as part of a subsequent release of this documentation.

2.6 Impacts from further regulations

This chapter will be provided as part of a subsequent release of this documentation.

2.7 Assumptions and justifications

This chapter will be provided as part of a subsequent release of this documentation.

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 2.1.1. 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 Appendix A. Figure 6 shows the proposed building blocks from a hardware and Figure 7 from a functional / software point of view.

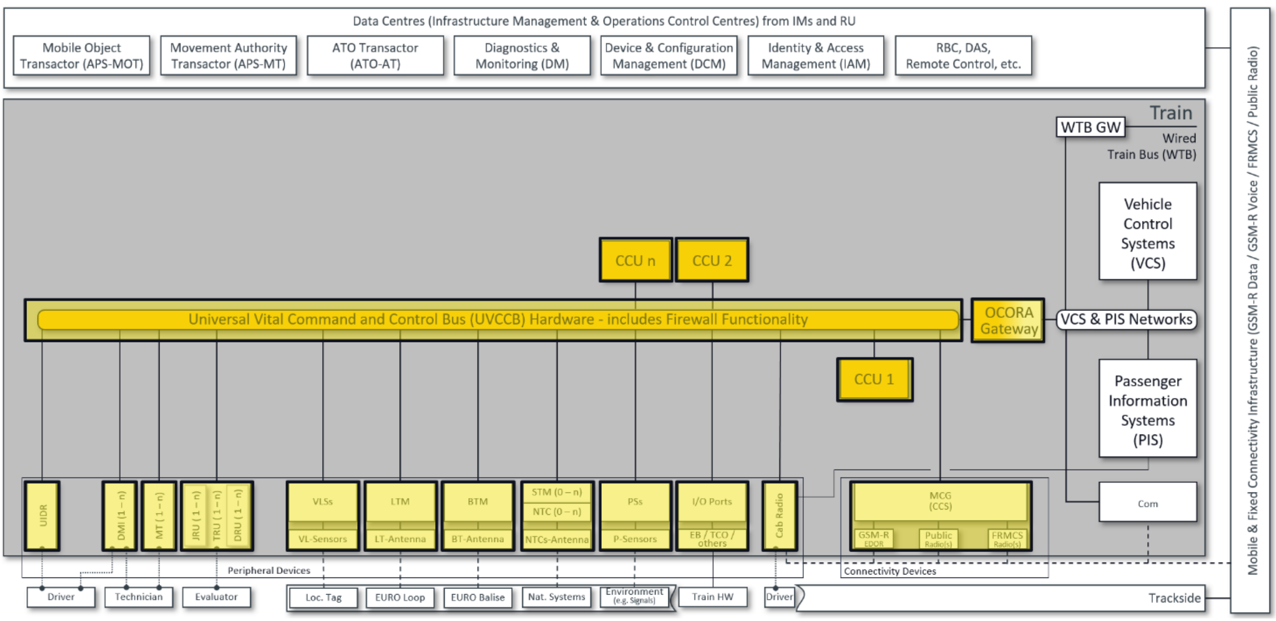

Figure 6 Hardware building blocks (tentative)

OCORA aims at defining the interfaces between the hardware building blocks and the functional and non-functional requirements of each building block. This ensure “plug & play”-like exchangeability of every building block.

Refer to chapter 4.1, 4.2, and 4.3 for a high level description of the identified hardware components.

OCORA also aims at defining the interfaces between the software building blocks and the functional and non-functional requirements of each software building block. This ensure “plug & play”-like exchangeability of every software building block. Although many functional components are grouped into the “ETCS Core” building block, OCORA may still demand a modular SW architecture within this block through non-functional requirements.

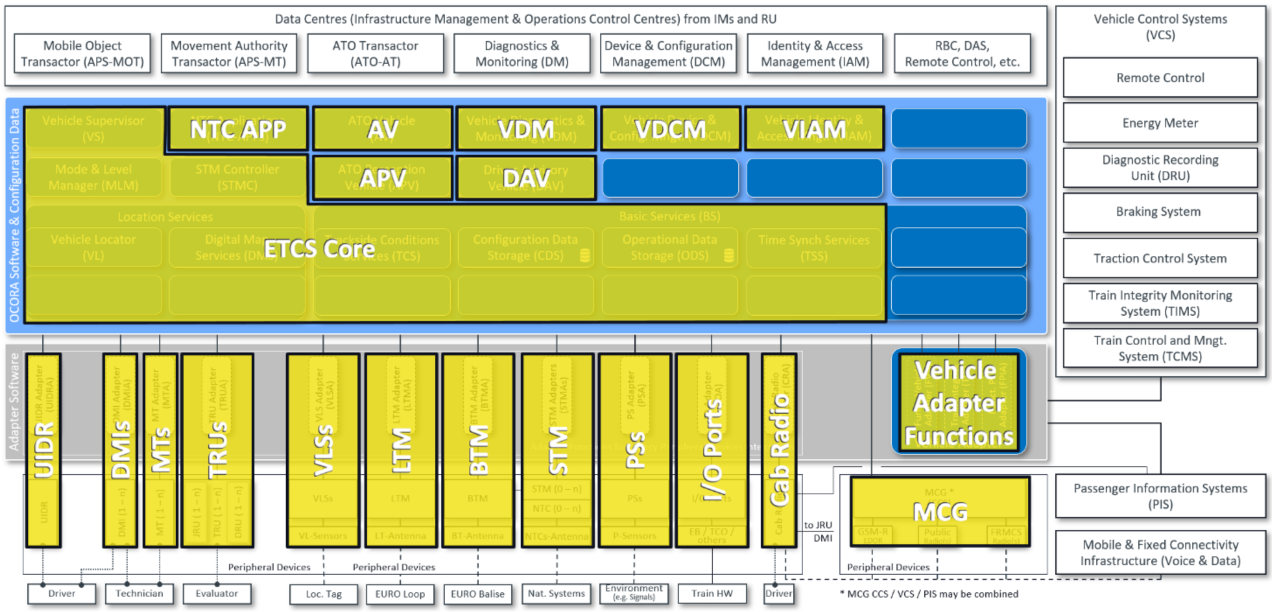

Figure 7 Functional / software building blocks (tentative)

Eventually, a separation of CCU hardware from software is envisioned as outlined in chapter 7. As a result, there will be no dependency between CCU hardware and OCORA software anymore. The “Runtime Environment” (refer to chapter 7) acts as hardware abstraction and may be bundled with the hardware.

Refer to chapter 4.4, 4.4.11, and 4.5 for a more detailed description of the identified functional components.

4 Component description

4.1 OCORA core hardware

The OCORA core hardware are the components within the "OCORA Core" scope. For these components, OCORA not provides interface specifications, high-level functional requirements, and non-functional requirements. The OCORA core hardware is also considered for all RAMSS aspects.

The OCORA core hardware, together with the runtime environment (refer to chapter 7), provides the platform to run the OCORA core functionality.

4.1.1 Universal Vital Command and Control Bus (UVCCB)

The Universal Vital Command and Control Bus (UVCCB) is the CCS on-board bus/network allowing direct communication between all CCS on-board components connected to it and eventually with external systems, such as the TCMS. The UVCCB 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 UVCCB is a TSN Ethernet based network with the use of SDTv2/v4 as safety layer. The bus/network is currently defined for OSI layer 1 to 2 and to a certain extent for OSI layer 3 to 5 (refer to OCORA OSI definitions in document [7]). At the final stage the UVCCB will be specified up to OSI layer 6 and 7 (refer to OCORA OSI definitions in document [7]) in subsequent versions of the OCORA specifications. Refer to Appendix C for a detailed discussion on the network topology scenarios that OCORA considers for implementing the UVCCB.

The UVCCB is installed on every OCORA based CCS on-board system. Refer to Appendix G1 on page 96 to locate the UVCCB component in the OCORA architecture.

Every CCS on-board device with high RAMS requirements has two TSN capable Ethernet ports. Refer to Appendix C for network topology scenarios.

On layer 3 to 6 at least IPv4, UDP, TCP and TRDP must be supported in order to be able to communicate directly to the TCMS. For communication between CCS on-board devices, other protocols on session layer are possible (e.g. OPC-UA Pub/Sub or DDS-RTPS).

Information regarding the requirements used for evaluating the UVCCB and the respective evaluation can be found in document [9].

Further details, especially the integration of the UVCCB with the NG-TCN and further investigations on OSI layer 3 to 6 (refer to OCORA OSI definitions in document [7]) are discussed in Appendix C and document [9].

4.1.2 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 7 for details).

At least one CCU is installed on every OCORA based CCS on-board system. Refer to Appendix G1 on page 96 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.

4.1.3 OCORA Gateway (OCORA-GW)

The OCORA Gateway (OCORA-GW) is a piece of hardware providing communication capabilities between the UVCCB (CCS-ECN) 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 [7]). 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 VCS/PIS networks are using the same technology, The OCORA-GW is not needed, and an ECN/ECN 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/bus is available. In case there is no TCMS the OCORA-GW can integrate directly with vehicle I/Os via the FVA located on the OCORA-GW. Refer to Appendix G1 on page 96 to locate the OCORA-GW component in the OCORA architecture.

Furthermore, the Passenger Information bus, 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 and PIS interface defined, the need for adapters vanishes and the Gateway may be reduced to a router or switch, hosting the needed firewalls (if not part of the on-board network components) and supporting the "plug & play"-like exchangeability of the UVCCB without reassessment of the TCMS segment in case of changes. For the interface with the vehicle TCMS, this is specified in document [11], [12] and [13].

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 G1 on page 96, 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.

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.

4.2.1 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 G1 on page 96 to locate the UIDR component in the OCORA architecture.

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

4.2.2 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 Voice, 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 G1 on page 96 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.

4.2.3 Maintenance Terminal (MT)

The Maintenance Terminal (MT) is a laptop that can be connected to the UVCCB 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 G1 on page 96 to locate the MT components in the OCORA architecture.

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

4.2.4 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 G1 on page 96 to locate the TRU components in the OCORA architecture.

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

4.2.5 Vehicle Localisation Systems (VLSs)

The Vehicle Localisation Systems (VLSs) processes the data from the various Vehicle Localisation Sensors, performs the necessary sensor fusion, and provides the data to the VL through the UVCCB.

At least one VLS is installed on every OCORA based CCS on-board system. The sensors connected to it may differ from one installation to the other. The architecture allows to install multiple VLSs to support different type of sensors, if needed (e.g. separate VLS for IMU sensors). Refer to Appendix G1 on page 96 to locate the VLS component in the OCORA architecture.

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

4.2.6 Vehicle Localisation Sensors (VL-Sensors)

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

VL 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 G1 on page 96 to locate the VL-Sensor component in the OCORA architecture.

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

4.2.7 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 UVCCB.

The LTM is installed on every OCORA based CCS on-board system in need Euroloop functionality. Refer to Appendix G1 on page 96 to locate the LTM component in the OCORA architecture.

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

4.2.8 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 G1 on page 96 to locate the LT-Antenna component in the OCORA architecture.

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

4.2.9 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 UVCCB, for the ETCS application (VS). Optionally, the BTM can also receive data from KER Balises and can make the data available, through the UVCCB, to the corresponding STM through the K interface describe in SUBSET-101.

The BTM is installed on every OCORA based CCS on-board system in need of ETCS functionality. Refer to Appendix G1 on page 96 to locate the BTM component in the OCORA architecture.

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

4.2.10 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 can 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 G1 on page 96 to locate the BT-Antenna component in the OCORA architecture.

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

4.2.11 Specific Transmission Module (STM)

The Specific Transmission Module (STM) provides the connection between the ETCS system (in case of OCORA the UVCCB) 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.

Multiple STMs can be connected to the UVCCB. They are installed on OCORA based CCS on-board system on an as needed basis. Refer to Appendix G1 on page 96 to locate the STM components in the OCORA architecture.

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

4.2.12 National Train Control (NTC)

The National Train Control (NTC) provides Automated Train Protection functionality on national level. It communicates with other OCORA components, namely the STM Controller (STMC) and can also use the functionality of other components connected to the UVCCB (e.g. DMI, VLS, TCO, EB, etc.). Alternatively, it is also possible to implement the National Train Controls business logic as Applications on the OCORA computing platform (see NTC-APPs for more information). In this case, the NTC-APPs access through the UVCCB and the BTM the balise data in order to get the packet 44 information.

Multiple NTCs can be connected via the respective STM to the UVCCB. They are installed on OCORA based CCS on-board system on an as needed basis. Refer to Appendix G1 on page 96 to locate the NTC components in the OCORA architecture.

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

4.2.13 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 UVCCB. They are installed on OCORA based CCS on-board system on an as needed basis. Refer to Appendix G1 on page 96 to locate the NTC-Antenna components in the OCORA architecture.

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

4.2.14 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 UVCCB.

The PSs are installed on OCORA based CCS on-board system, if needed for ATO GoA1 – GoA4 operations. Refer to Appendix G1 on page 96 to locate the PSs component in the OCORA architecture.

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

4.2.15 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, but can also include vibration sensors, smoke detectors, etc.

The P-Sensors are installed on OCORA based CCS on-board system, supporting ATO GoA1 – GoA4. Refer to Appendix G1 on page 96 to locate the P-Sensor components in the OCORA architecture.

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

4.2.16 I/O Ports

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

The I/O Ports are installed on every OCORA based CCS on-board system. Refer to Appendix G1 on page 96 to locate the I/O Ports component in the OCORA architecture.

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

4.2.17 Emergency Brake (EB) / Traction Cut-Off (TCO) / Others

These are the devices triggering the Emergency Brake (EB) and the Traction Cut-Off (TCO) for ETCS, NTC-APP, APV, etc. Depending on the system configuration and RU's need, multiple EBs and TCOs can be connected and additional I/Os can be used to interact with "other" external systems, actuators, and sensors. Examples are:

- *Cabin activation status*
- *ETCS isolation status*
- *Vehicle power status*
- *Dead Man Switch: to monitor the awareness of the driver*
- *CCS Cabinet Supervision: to monitor unauthorized access*

At least one EB and TCO devices are installed on every OCORA based CCS on-board system, as long as the TCMS does not provide SIL4 functionality for TCO and EB activation. Refer to Appendix G1 on page 96 to locate the EB and TCO components in the OCORA architecture.

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

4.2.18 Cabin Radio

The Cabin Radio 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 HMI, 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 Cab Radio 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 between the CCS data and cabin voice. The OCORA concept foresees providing voice communication through voice over IP (VoIP) and to connect to the PIS, DMI and the JRU through the UVCCB.

The Cabin Radio is an optional deployment on OCORA based CCS on-board system. Refer to Appendix G1 on page 96 to locate the Cabin Radio device in the OCORA architecture.

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

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 C for a discussion of possible options.

4.3.1 Mobile Communication Gateway (CCS) (MCG (CCS))

The Mobile Communication Gateway (MCG (CCS)) provides train to track-side communication for the on-board CCS and depending on the vehicle, it may also provide track-side connectivity for the systems of the Train Control bus (VCS and PIS). The GSM-R and the FRMCS Radio will be either part of the MCG (CCS) or will be connected to the MCG (CCS), providing 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.

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) acts also as a firewall for all communications between trackside and-on-board networks.

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.

There are several possible scenarios for the network topology and where to connect the MCG (CCS) to the on-board network(s). Appendix C provides a detailed explanation and a view in relation to the OSI Layers and the cyber security aspects for the different scenarios and a discussion for the evaluation of the preferable scenario against a weighted set of criteria.

#	Title	Description
1	**Legacy Train / MCG connected to UVCCB**	The CCS Network is running on the OCORA UVCCB and is connected to a legacy vehicle using the OCORA-GW for physical and logical adaptation. The MCG is connected to the UVCCB providing mobile communication between trackside and on-board networks. **Remark:** This scenario will not be evaluated against the others, since it is related to the integration into an existing train with a legacy network technology.
2	**Separate Networks / MCG connected to UVCCB**	The CCS and the TCMS are running on physically separated Ethernet Consist Networks (ECN) and are interconnected through a gateway providing routing and cyber security functionality between the two networks. **The MCG is connected to the UVCCB** providing mobile communication between trackside and on-board networks.
2a	**Separate Networks / MCG connected to the TCN**	The CCS and the TCMS are running on physically separated Ethernet Consist Networks (ECN) and are interconnected through a gateway providing routing and cyber security functionality between the two networks. **The MCG is connected to the TCN** providing mobile communication between trackside and on-board networks.
2b	**Separate Networks / MCG on both Networks**	The CCS and the TCMS are running on physically separated Ethernet Consist Networks (ECN) and are interconnected through a gateway providing routing and cyber security functionality between the two networks. **There is a separate MCG on each network** providing mobile communication between trackside and the particular on-board network.
3	**Common Network / MCG on common Network**	The CCS and TCMS are using the same network technology and therefore the MCG is part of the common network providing trackside connectivity to all on-board systems.

Table 9 Possible scenarios for the network topology and where to connect MCG

At this point in time a first list of evaluation criteria is available (see table below). It consists of the OCORA design principles, the RAMS aspects, and the market readiness.

Criteria	Weight	1	2	2a	2b	3
Openness		n/a				
Modularity		n/a				
Exchangeability		n/a				
Migrateability		n/a				
Evolvability		n/a				
Portability		n/a				
Security		n/a				
Reliability		n/a				
Availability		n/a				
Maintainability		n/a				
Total						

Table 10 Evaluation of connectivity scenarios (to be filled-in subsequent releases)

4.3.2 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 eventually be replaced by an FRMCS Radio.

The GSM-R EDOR Radio is installed on every OCORA based CCS on-board system supporting ETCS L2 or higher, as long as FRMCS is not widely deployed. Refer to Appendix G1 on page 96 to locate the GSM-R EDOR Radio component in the OCORA architecture.

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

4.3.3 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, 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 G1 on page 96 to locate the Public Radio component in the OCORA architecture.

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

4.3.4 Future Rail Mobile Communication System (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, once FRMCS is available. Refer to Appendix G1 on page 96 to locate the FRMCS Radio components in the OCORA architecture.

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

4.4 OCORA software and configuration data

The OCORA software and configuration data provides the actual (business) logic and configuration data for the CCS on-board functions and functionality to be able perform maintenance tasks efficiently. At the current stage, a set of software components are identified. However, more software components will be defined in subsequent versions of this document. But the OCORA platform also provides an API that allows new software components, not known at this point in time, to use the services of the platform and the infrastructure of the vehicle. Hence, developing and deploying new functionality should be simplified. Such software components could be "automated routine test" or an NTC application that uses balise data, packet 44.

All OCORA software components run on the OCORA computing platform (refer to chapter 7).

4.4.1 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.

The VS application is deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 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.

4.4.2 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 G2 on page 97 to locate the MLM component in the OCORA architecture. In today's ETCS implementations, the MLM is part of the monolithic ETCS OBU.

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

4.4.3 National Train Control Applications (NTC-APPs)

The National Train Controls Applications (NTC-APPs), deployed on the OCORA computing platform, are safe applications in charge of ensuring automated train protection based on national systems. NTC-APPs, implemented on the OCORA computing platform, must communicate, as a minimum, with the ATP Manager 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 TRU, DMI can be used, the TCMS can be accessed through the Functional Vehicle Adapter (FVA), etc.

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 G2 on page 97 to locate the NTC-APPs in the OCORA architecture.

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

4.4.4 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 automated 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 G2 on page 97 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.

4.4.5 ATO Vehicle (AV)

The ATO Vehicle (AV) application, deployed on the OCORA computing platform, is a non-safe application for automated train operations. A safe extension is needed for GoA3 and GoA4 operations. This is provided by the ATO Perception Vehicle (APV). 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 G2 on page 97 to locate the AV component in the OCORA architecture.

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

4.4.6 ATO Perception Vehicle (APV)

The ATO Perception Vehicle (APV) application, deployed on the OCORA computing platform, is a safe application needed for automated train operations with GoA3 and GoA4. In case of light signalling perception, the APV may also be used in GoA2. It is deployed in addition to ATO Vehicle (AV) and includes all safety-related functionality and data needed for GoA3 and GoA4 operations. To execute these tasks, it has interfaces to perception system, Digital Maps (DMS), etc. Based on the situation (type of danger and location information) it triggers speed reduction, service brakes, traction cut-off, pantograph drop, horn, and emergency brakes. Remark: APV is called "Incident Protection Management" (IPM) in GoA3 – GoA4 Shift2Rail discussions. There is an open possibly that APV may be indirectly linked – through a Signalling ConVerter (SCV) - to the VS in order to emulate lateral signalling into ETCS messages.

The APV application is deployed on every OCORA based CCS on-board system in need of ATO GoA3 or GoA4 functionality. In case of light signalling perception, the APV may also be used for GoA1-2 operations. Refer Appendix G2 on page 97 to locate the APV component in the OCORA architecture.

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

4.4.7 Driver Advisory Vehicle (DAV)

The Driver Advisory Vehicle (DAV) application 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) or the Traffic Management System (TMS) is responsible for conflict detection and calculation of new target train timings, that are forwarded to the DAV and evaluated accordingly. The typical integration of DAV application is defined EN 15380-4. The DAV can also operate standalone (e.g. without integration into the vehicle). The DAV is not needed if ATO Vehicle (AV) is installed, since the AV already includes the DAV functionality. The implementation of DAV application on 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 G2 on page 97 to locate the DAV component in the OCORA architecture.

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

4.4.8 Vehicle Diagnostic & Monitoring (VDM)

The Vehicle Diagnostics & Monitoring (VDM) service, 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 standardized format. For remote diagnostics and monitoring the data can be send 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). While the TRUA provides the data for recording in the TRU, the VDM provides the data to other systems such as the centralized DMs or the Maintenance Terminals.

The VDM service is foreseen to be deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 to locate the VDM component in the OCORA architecture.

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

4.4.9 Vehicle Device & Configuration Management (VDCM)

The Vehicle Device & Configuration Management (VDCM) service, deployed on the OCORA computing platform, allows for local (through the Maintenance Terminal) and remote (through the centralized 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).

The VDCM service is foreseen to be deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 to locate the VDCM component in the OCORA architecture.

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

4.4.10 Vehicle Identity & Access Management (VIAM)

The Vehicle Identity & Access Management (VIAM) 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 application 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 UVCCB 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 unauthorized access to resources and functions within the CCS on-board system.

The VIAM service is foreseen to be deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 to locate the VIAM component in the OCORA architecture.

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

4.4.11 Location Services (LS)

4.4.11.1 Vehicle Locator (VL)

The Vehicle Locator (VL) is a safe service deployed on the OCORA computing platform. It provides the actual position/direction in relation to infrastructure elements to the VS, where the actual position/direction and the current speed are aggregated with other data into a Train Position Report (TPR). Localisation data may be sent by the VL to APS-MOT, containing e.g. ETCS irrelevant data (not used by VS). The VL sends the full virtual track occupation of the train or only a part of it (only the front or rear position). The VL can use different localization technologies, from today's "balise + odometry" to additional sensor inputs such as GNSS or inertial measurement units. To access the respective sensors, the VL interacts with the Vehicle Localisation Systems (VLSs).

The VL service is deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 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 D 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 will be provided in subsequent versions of the OCORA architecture documentation.

4.4.11.2 Digital Map Services (DMS)

The Digital Map Service (DMS) is a safe service deployed on the OCORA computing platform. The DMS 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, APV) 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 DMS uses its own on-board data storage that is updated, if required, using the functionality of the Vehicle Device & Configuration Management (VDCM) to propagate trackside map data (e.g. from Topo4) to the on-board data storage.

The DMS is foreseen to be deployed on every OCORA based CCS on-board system in need of GoA3 – GoA4 functionality or if the VLS has a need for it. In case of light signalling perception, the DMS may also be used for GoA1-2 operations. Refer to Appendix G2 on page 97 to locate the DMS 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 (DMS) 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 geo-referenced 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.

4.4.12 Basic Services (BS)

4.4.12.1 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 through IF490 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 G2 on page 97 to locate the TCS component in the OCORA architecture.

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

4.4.12.2 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. VDM). 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 Vehicle Device & Configuration Management (VDCM) 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 G2 on page 97 to locate the CDS component in the OCORA architecture.

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

4.4.12.3 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, 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 G2 on page 97 to locate the ODS component in the OCORA architecture.

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

4.4.12.4 Time Synch Services (TSS)

The Time Synchronisation Service (TSS) provides a service that allows all on-board components to have their time in synch with each other and synched with the trackside systems (e.g. safe data centres). The time base is UTC and components in need to display the time can revert it to local time. This functionality is significant to simplify diagnostic and analysis, for ATO operations, and other aspects.

The TSS is foreseen to be deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 to locate the TSS component in the OCORA architecture.

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

4.5 Adapter software

The adapter software contains software components that allow abstracting the different type of train hardware towards the standard OCORA software. The goal of these software components is to ensure that the interfaces with the OCORA software remain the same, regardless of the underlying train hardware.

The adapter software components run on the peripheral devices, or on a specific adapter hardware, or, in some cases, on the OCORA Gateway.

4.5.1 Functional Vehicle Adapter (FVA)

The Functional Vehicle Adapter (FVA) is a piece of software deployed on the OCORA computing platform, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardized interface towards the CCS applications and services for vehicle functions and vehicle information needed by the OCORA on-board applications and services. Although the TSI-CCS SUBSET-034, SUBSET-119, and SUBSET-139 are defining the interface to the TCMS system, vehicle 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. In addition, the FVA can also be used to integrate vehicles through wired connections. Also, the standardized interface to the CCS applications evolves in multiple iterations as outlined in chapter 3. 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 other context a piece of hardware is meant. To avoid confusion, OCORA does not use the term TIU.

The FVA component is foreseen to be deployed on every OCORA based CCS on-board system as long as there is no common standard TCMS interface, that is the same for all trains. Refer to Appendix G2 on page 97 to locate the FVA component in the OCORA architecture.

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

4.5.2 Train Integrity Adapter (TIA)

The Train Integrity Adapter (TIA) is a safe piece of software 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 service 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 standardized interface, independent of the option used. The train integrity status may also include the total safe train length (including the length over coupled compositions).

The TIA adapter is deployed on every OCORA based CCS on-board system in need of ETCS L3 functionality. Refer to Appendix G2 on page 97 to locate the TIA software component in the OCORA architecture

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

4.5.3 Functional Passenger Information System Adapter (FPIA)

The Functional Passenger Information Adapter (FPIA) 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 standardized interface towards the Passenger Information System (PIS), allowing the PIS to receive CCS of interest to the PIS.

The FPIA component is foreseen to be deployed on every OCORA based CCS on-board system. Refer to Appendix G2 on page 97 to locate the FPIA component in the OCORA architecture.

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

5 External interfaces of the “CCS On-Board” scope

This chapter identifies and describes all interfaces for the “CCS On-Board” scope. The content in this chapter represents the current state of work. The chapter will evolve over subsequent versions of this document.

5.1 Mechanical interfaces

Information will be provided in subsequent versions of this document.

5.2 Electrical interfaces

Information will be provided in subsequent versions of this document.

5.3 Communication interfaces (OSI layers 1-6)

The following pictures identify all communication interface for OSI layers 1-6 (refer to OCORA OSI definitions in document [7]) for the “CCS On-Board” scope. The table following the graphics provides a high-level description for every interface.

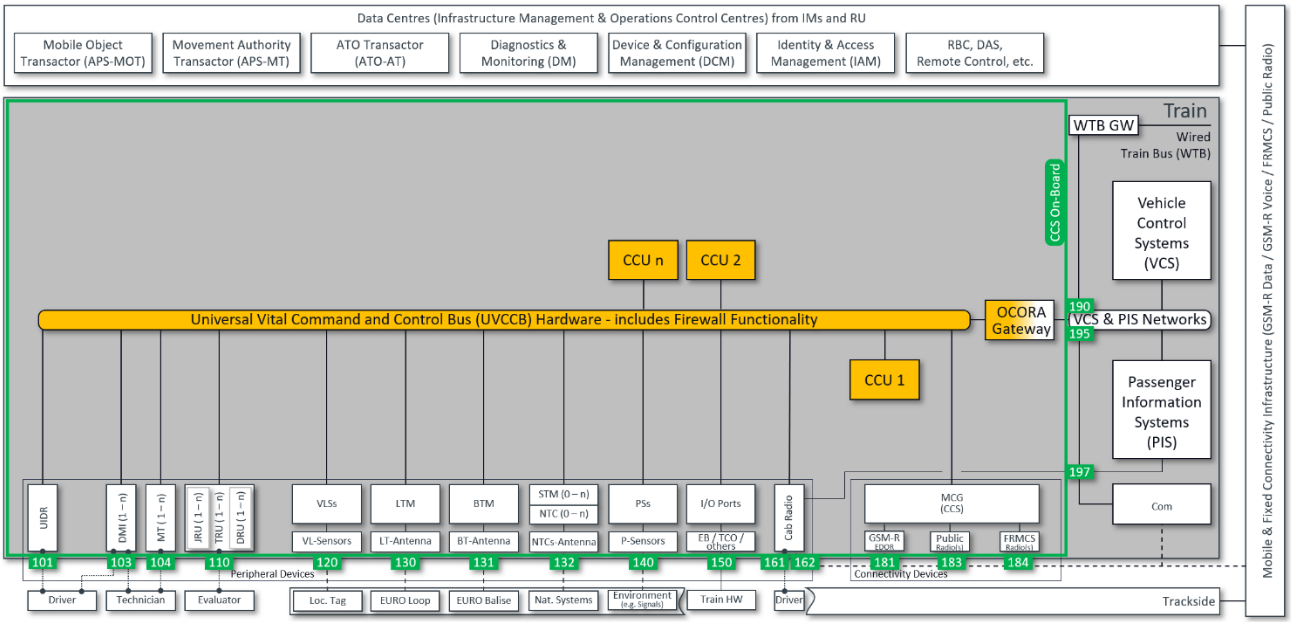

Figure 8 “CCS On-Board” hardware with external communication IFs OSI layers 1-6

Interface ID	High-Level Description
101	This is the interface between the User Identification Reader (refer to chapter 4.2.1) and the Driver or the Driver's UID card (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
103	This is the interface between the Driver Machine Interface (refer to chapter 4.2.2) and the Driver or the Technician (refer to chapter 2.1.3.1). Standardization efforts for ETCS functionality are ongoing by the ERA (refer to document 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.
104	This is the interface between the Maintenance Terminals (refer to chapter 4.2.3) and the Technician (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
110	This is the interface between the Train Recording Units (refer to chapter 4.2.4) and the Evaluator (refer to chapter 2.1.3.1). 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.
120	These are the interface between the Vehicle Location Sensors (refer to chapter 4.2.6) and their environment that can include a trackside mounted Location Tag (refer to chapter 2.1.3.2). OCORA does not aim to standardize these interfaces. OCORA expects various technologies to be used.
130	This is the interface between the Loop Transmission Antenna (refer to chapter 4.2.8) and the EURO Loop (refer to chapter 2.1.3.2). SUBSET-044 specifies this interface.
131	This is the interface between the Balise Transmission Antenna (refer to chapter 4.2.10) and the EURO Balise (refer to chapter 2.1.3.2). SUBSET-036 specifies this interface.
132	This is the interface between the National Systems Antenna (refer to chapter 4.2.13) and the National Systems (refer to chapter 2.1.3.2). This is a specific interface of the existing ATP systems and is therefore not relevant for OCORA.
140	These are the interface between the Perception Sensors (refer to chapter 4.2.15) and their environment. OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
150	These are the interface between the Emergency Brake device / Traction Cut-off device / other devices (refer to chapter 4.2.17) and the respective vehicle infrastructure. This are existing discrete interfaces. OCORA does not aim to standardize these interfaces.
161	This is the interface between the Cabin Radio (refer to chapter 4.2.18) and the Driver (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
162	This is the GSM-R Voice interface between the Cabin Radio (refer to chapter 4.2.18) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). This interface is defined in the GSM-R specifications (EIRENE FRS v8.0.0 / SRS v16.0.0), developed under the EIRENE project and maintained by the UIC.
181	This is the interface between the GSM-R EDOR Radio (refer to chapter 4.3.1) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). This interface is defined in the GSM-R specifications (EIRENE FRS v8.0.0 / SRS v16.0.0), developed under the EIRENE project and maintained by the UIC. SUBSET-037 specifies this interface on functional level.

Interface ID	High-Level Description
183	This is the interface between the Public Radio (refer to chapter 4.3.3) and the “Mobile & Fixed Connectivity Infrastructure” (refer to chapter 2.1.3.2). This interface is standardized through the LTE and 5G Standards developed by the 3rd Generation Partnership Project (3GPP).
184	This is the interface between the FRMCS Radio (refer to chapter 4.3.4) and the “Mobile & Fixed Connectivity Infrastructure” (refer to chapter 2.1.3.2). The FRMCS FRS and SRS are in progress at UIC in corporation with the TOBA working-group, which covers the specifications for the FRMCS on-board equipment. SUBSET-037 specifies this interface on functional level.
190	This is the interface between the OCORA Gateway (refer to chapter 4.1.3), if it exists and the “Train Control Network” (refer to chapter 2.1.3.2) with its Train Control System (TCMS). If the OCORA Gateway is not needed on a specific vehicle, then this interface is between the CCS on-board system and the TCMS. This is a specific interface of the respective train. Standards exists or are being developed with SUBSET-034, SUBSET-119, SUBSET-139, and SUBSET-143. But these standards are relevant for modern vehicles with a TCMS only. Remark: the TCMS side of the gateway is vendor specific for all retrofit projects. OCORA does not aim at standardizing this interface but foresees the OCORA-GW to adapt to any kind of vehicle. Also, OCORA is working together with the organization (S2R) that aims at standardizing this interface for modern vehicles.
195	This is the interface between the OCORA Gateway (refer to chapter 4.1.3), if it exists and the “Passenger Information Network” (refer to chapter 2.1.3.2) with its Passenger Information Systems (PISs). If the OCORA Gateway is not needed on a specific vehicle, then this interface is between the CCS on-board system and the PIS. OCORA may consider providing a standard for this interface at a later stage. The interface allows the PIS to get information from the CCS on-board system, such as speed, location, etc.
197	This is the UIC interface, allowing to communicate between the Cab Radio and the PIS. This interface may not be needed on modern trains, equipped with a NG-TCN. In these situations, the communication may be routed through the UVCCB (IF300).

Table 11 External communication IFs of the “CCS On-Board” scope (OSI layers 1-6)

5.4 Communication interfaces (OSI layer 7)

The following pictures identify all communication interface for OSI layer 7 (refer to OCORA OSI definitions in document [7]) for the “CCS On-Board” scope. The table following the graphics provides a high-level description for every interface.

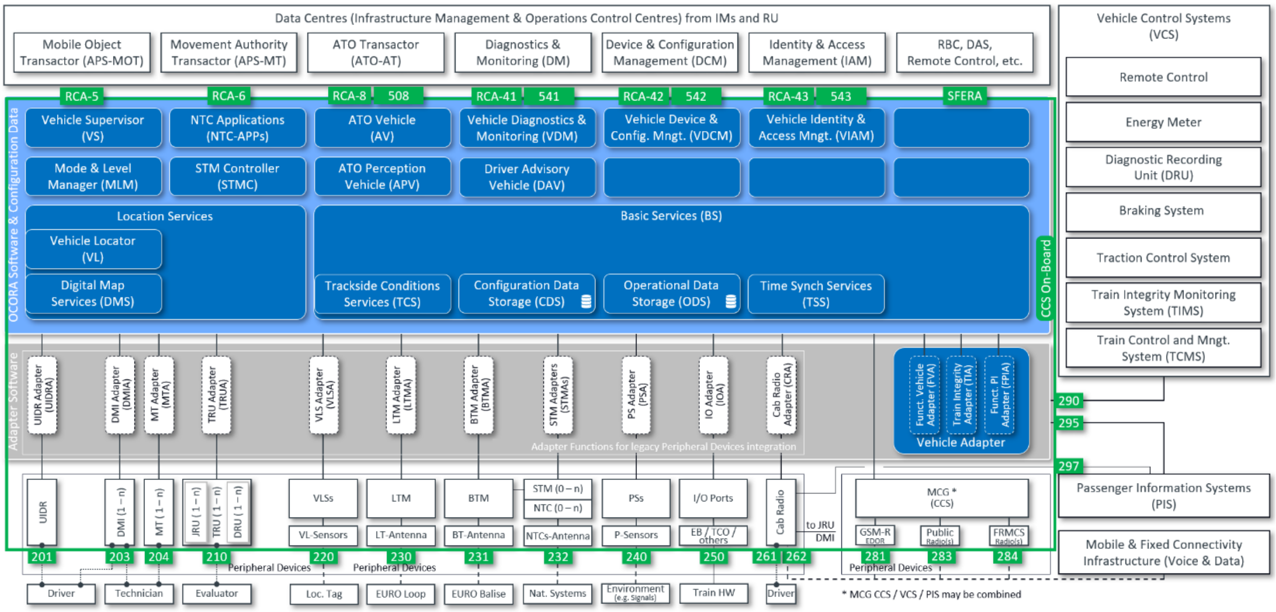

Figure 9 “CCS On-Board” software components with external communication Ifs OSI Layer 7

Interface ID	High-Level Description
201	This is the interface between the User Identification Reader (refer to chapter 4.2.1) and the Driver or the Driver’s UID card (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
203	This is the interface between the Driver Machine Interface (refer to chapter 4.2.2) and the Driver or the Technician (refer to chapter 2.1.3.1). Standardization efforts for ETCS functionality are ongoing by the ERA (refer to document 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.
204	This is the interface between the Maintenance Terminals (refer to chapter 4.2.3) and the Technician (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
210	This is the interface between the Train Recording Units (refer to chapter 4.2.4) and the Evaluator (refer to chapter 2.1.3.1). 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.
220	These are the interface between the Vehicle Location Sensors (refer to chapter 4.2.6) and their environment that can include a trackside mounted Location Tag (refer to chapter 2.1.3.2). OCORA does not aim to standardize these interfaces. OCORA expects various technologies to be used.

Interface ID	High-Level Description
230	This is the interface between the Loop Transmission Antenna (refer to chapter 4.2.8) and the EURO Loop (refer to chapter 2.1.3.2). SUBSET-044 specifies this interface.
231	This is the interface between the Balise Transmission Antenna (refer to chapter 4.2.10) and the EURO Balise (refer to chapter 2.1.3.2). SUBSET-036 specifies this interface.
232	This is the interface between the National Systems Antenna (refer to chapter 4.2.13) and the National Systems (refer to chapter 2.1.3.2). This is a specific interface of the existing ATP systems and is therefore not relevant for OCORA.
240	These are the interface between the Perception Sensors (refer to chapter 4.2.15) and their environment. OCORA does not aim to standardize these interfaces. But standards may be needed at some point in time.
250	These are the interface between the Emergency Brake device / Traction Cut-off device / other devices (refer to chapter 4.2.17) and the respective vehicle infrastructure. This are existing discrete interfaces. OCORA does not aim to standardize these interfaces.
261	This is the interface between the Cabin Radio (refer to chapter 4.2.18) and the Driver (refer to chapter 2.1.3.1). OCORA does not aim to standardize this interface.
262	This is the interface between the Cabin Radio (refer to chapter 4.2.18) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). This interface is defined in the GSM-R specifications (EIRENE FRS v8.0.0 / SRS v16.0.0), developed under the EIRENE project and maintained by the UIC.
281	This is the interface between the GSM-R EDOR Radio (refer to chapter 4.3.1) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). This interface is defined in the GSM-R specifications (EIRENE FRS v8.0.0 / SRS v16.0.0), developed under the EIRENE project and maintained by the UIC. SUBSET-037 specifies this interface on functional level.
283	This is the interface between the Public Radio (refer to chapter 4.3.3) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). This interface is standardized through the LTE and 5G Standards developed by the 3rd Generation Partnership Project (3GPP).
284	This is the interface between the FRMCS Radio (refer to chapter 4.3.4) and the "Mobile & Fixed Connectivity Infrastructure" (refer to chapter 2.1.3.2). The FRMCS FRS and SRS are in progress at UIC in corporation with the TOBA working-group, which covers the specifications for the FRMCS on-board equipment. SUBSET-037 specifies this interface on functional level.
290	This is the interface between the OCORA Gateway (refer to chapter 4.1.3), if it exists and the "Train Control Network" (refer to chapter 2.1.3.2) with its Train Control System (TCMS). If the OCORA Gateway is not needed on a specific vehicle, then this interface is between the CCS on-board system and the TCMS. On a functional level (OSI layer 7, refer to OCORA OSI definitions in document [7]), this is the interface between the Functional Vehicle Adapter and the TCMS or whatever system exists on the train side. This is a specific interface of the respective train. Standards exists or are being developed with SUBSET-034, SUBSET-119, SUBSET-139, and SUBSET-143. But these standards are relevant for modern vehicles with a TCMS only. Remark: the TCMS side of the gateway is vendor specific for all retrofit projects. OCORA does not aim at standardizing this interface but foresees the OCORA-GW to adapt to any kind of vehicle. Also, OCORA is working together with the organization (S2R) that aims at standardizing this interface for modern vehicles.

Interface ID	High-Level Description
295	This is the interface between the OCORA Gateway (refer to chapter 4.1.3), if it exists and the "Passenger Information Network" (refer to chapter 2.1.3.2) with its Passenger Information Systems (PISs). If the OCORA Gateway is not needed on a specific vehicle, then this interface is between the CCS on-board system and the PIS. OCORA may consider providing a standard for this interface at a later stage. The interface allows the PIS to get information from the CCS on-board system, such as speed, location, etc.
297	This is the UIC interface, allowing to communicate between the Cab Radio and the PIS. This interface may not be needed on modern trains, equipped with a NG-TCN. In these situations, the communication may be routed through the UVCCB (IF300) and the IF295.
RCA-5	This is the interface between the Vehicle Locator (refer to chapter 4.4.11.1) and the Advanced Protection System's Mobile Object Transactor (refer to chapter 2.1.3.2). This information is used by the VL to send localisation data to the APS-MOT, containing e.g. ETCS irrelevant data (not used by VS). This interface is being standardized by RCA.
RCA-6	This is the interface between the Vehicle Supervisor (refer to chapter 4.4.1) and the Advanced Protection System's Movement Authority Transactor (refer to chapter 2.1.3.2) or the Radio Block Center, depending on the system provided by the infrastructure manager. SUBSET-026, chapter 7 & 8 define this interface.
RCA-8	This is the interface between the ATO Vehicle (refer to chapter 4.4.5) and the ATO Transactor (refer to chapter 2.1.3.2). SUBSET-126 is being prepared by S2R to specify this interface.
508	This is the interface between the ATO Vehicle (refer to chapter 4.4.5) and the ATO Transactor from the RU. This is only needed when no driver is present (GoA 3 – 4) for driving trains outside the timetable (e.g. to the depot).
RCA-41	This is the interface between Vehicle Diagnostic & Monitoring (refer to chapter 4.4.8) and the Diagnostic & Monitoring system (refer to chapter 2.1.3.2) of the infrastructure manager, the vehicle currently operates in. This interface is defined by RCA. Refer to document [18].
541	This is the interface between Vehicle Diagnostic & Monitoring (refer to chapter 4.4.8) and the Diagnostic & Monitoring system (refer to chapter 2.1.3.2) of the railway undertaking. OCORA aims at providing a standard for this interface.
RCA-42	This is the interface between Vehicle Device & Configuration Management (refer to chapter 4.4.9) and the Device & Configuration Management system (refer to chapter 2.1.3.2) of the infrastructure manager, the vehicle currently operates in. This interface is defined by RCA. Refer to document [18].
542	This is the interface between Vehicle Device & Configuration Management (refer to chapter 4.4.9) and the Device & Configuration Management system (refer to chapter 2.1.3.2) of the railway undertaking. OCORA aims at providing a standard for this interface.
RCA-43	This is the interface between Vehicle Identity & Access Management (refer to chapter 4.4.10) and the Identity & Access Management system (refer to chapter 2.1.3.2) of the infrastructure manager, the vehicle currently operates in. This interface is defined by RCA. Refer to document [18].
543	This is the interface between Vehicle Identity & Access Management (refer to chapter 4.4.10) and the Identity & Access Management system (refer to chapter 2.1.3.2) of the railway undertaking. OCORA aims at providing a standard for this interface.
SFERA	This is the interface between Driver Advisory Vehicle (refer to chapter 4.4.7) and the Driver Advisory System (refer to chapter 2.1.3.2) of the railway undertaking. SFERA aims at providing a standard for this interface.

Table 12 External communication IFs of the "CCS On-Board" scope (OSI layer 7)

6 External interfaces of the “OCORA Core” scope

This chapter identifies and describes all interfaces for the “OCORA Core” scope. The content in this chapter represents the current state of work. The chapter will evolve over subsequent versions of this document.

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 picture identifies all communication interface for OSI layers 1-6 (refer to OCORA OSI definitions in document [7]) for the “OCORA Core” scope. The table following the graphic provides a high-level description for every interface.

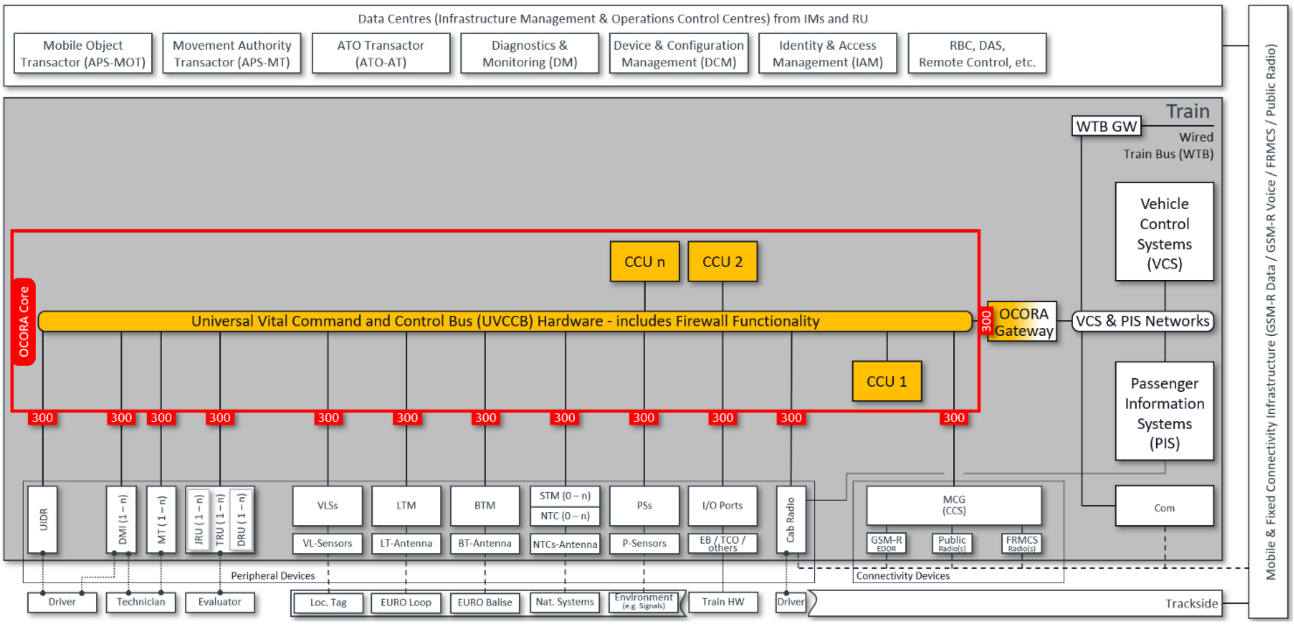

Figure 10 “OCORA Core” hardware with external communication IFs (OSI Layers 1-6)

Interface ID	High-Level Description
300	This is the interface, the Universal Vital Command and Control Bus (refer to chapter 4.1.1) provides to the CCUs (refer to chapter 4.1.2), the OCORA Gateway (refer to chapter 4.1.3), all the peripheral devices (refer to chapter 4.2), and possibly to the connectivity devices (refer to chapter 4.3). The interface is currently defined for OSI layer 1 to 2 (refer to OCORA OSI definitions in document [7]) but will be specified up to OSI layer 6 and 7 (refer to OCORA OSI definitions in document [7]) in subsequent versions of the OCORA specifications.

Table 13 External communication IFs of the “OCORA Core” scope (OSI layers 1-6)

6.4 Functional interfaces (OSI layer 7)

The following picture identifies all functional interface for OSI layer 7 (refer to OCORA OSI definitions in document [7]) for the “OCORA Core” scope. The table following the graphic provides a high-level description for every interface.

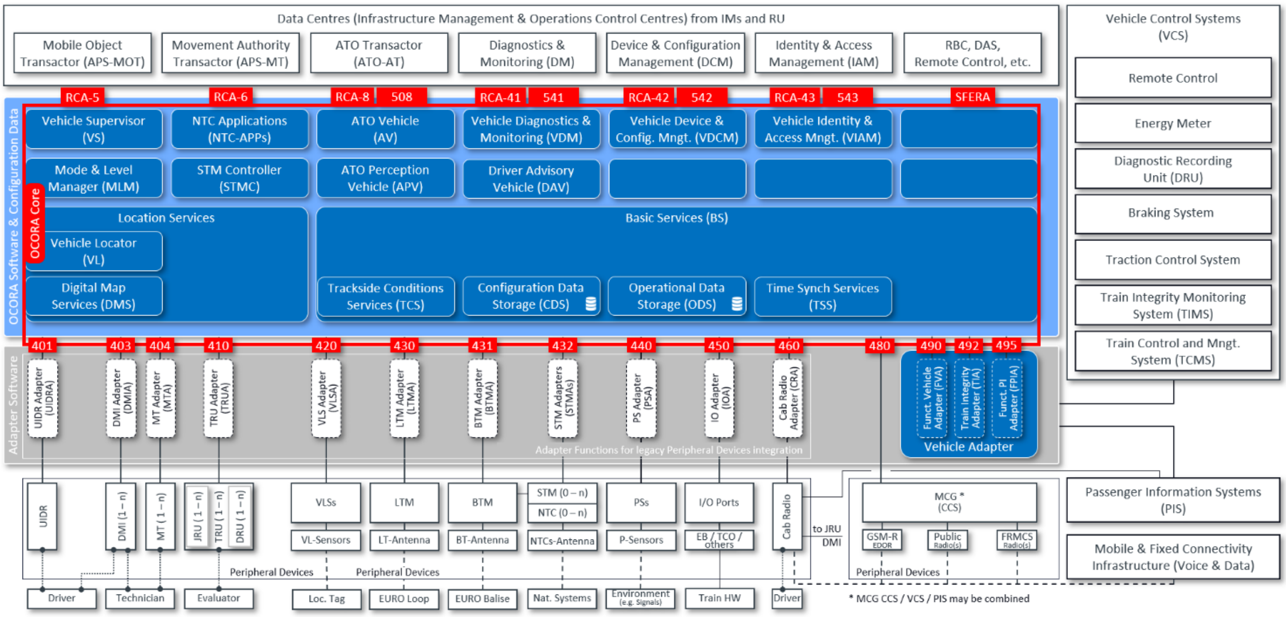

Figure 11 “OCORA Core” functional components with external communication IFs (OSI Layer 7)

Interface ID	High-Level Description
401	This is the functional interface between the User Identification Reader Adapter (UIDRA), if it exists or the User Identification Reader (UIDR) and the OCORA software. OCORA aims to provide a standard for this interface.
403	This is the functional interface between the Driver Machine Interface Adapter (DMIA), if it exists or the Driver Machine Interfaces (DMIs) and the OCORA software. SUBSET-121 aims at providing a standard. OCORA aims to define this interface exhaustively.
404	This is the functional interface between the Maintenance Terminal Adapter (MTA), if it exists or the Maintenance Terminals (MTs) and the OCORA software. OCORA aims to provide a standard for this interface.
410	This is the functional interface between the Train Recording Unit Adapter (TRUA), if it exists or the Train Recording Unit (TRU) and the OCORA software. SUBSET-027 defines this interface for the Juridical Recording Unit (JRU) and work on SUSET-140 is in progress for other data (e.g. ATO). OCORA may want to extend this interface to allow standardized data recording for other components.
420	This is the functional interface between the Vehicle Location System Adapter (VLSA), if it exists or the Vehicle Location Systems (VLAs) and the OCORA software. A proposal from the European Economic Interest groups (ERTMS User Group) exists (refer to document [20]) for standardizing part of this interface. OCORA aims to define this interface exhaustively.
430	This is the functional interface between the Loop Transmission Module Adapter (LTMA), if it exists or the Loop Transmission Modul (LTM) and the OCORA software. SUBSET-026, chapter 7 and chapter 8 contain the data to be transferred over this interface. OCORA plans to standardize this interface, based on the existing specifications.

Interface ID	High-Level Description
431	This is the functional interface between the Balise Transmission Module Adapter (BTMA), if it exists or the Balise Transmission Modul (BTM) and the OCORA software. SUBSET-026, chapter 7 and chapter 8 contain the data to be transferred over this interface. In addition, SUBSET-101 contains the data to communicate with the Specific Transmission Module (STM). OCORA plans to standardize this interface, based on the existing specifications.
432	This is the functional interface between the Specific Transmission Module Adapters (STMAs), if it exists or the Specific Transmission Modules (STMs) and the OCORA software. SUBSET-035 and SUBSET-058 contains the data to be transferred over this interface. In addition, SUBSET-101 contains the data to communicate with the Balise Transmission Module (BTM). OCORA plans to standardize this interface, based on the existing specifications.
440	This is the functional interface between the Perception System Adapter (PSA), if it exists or the Perception System (PS) and the OCORA software. This interface may also include signal perception information. Various organisations are working on this topic (e.g. Tauro WP4). OCORA does not plan to work on this interface for the time being but aims at standardizing this interface at the given time.
450	This is the functional interface between I/O Adapter (IOA), if it exists or the I/O Ports and the OCORA software. SUBSET-034, SUBSET-119 and proposed SUBSET-139 contain information regarding this interface. OCORA plans to standardize this interface, based on the existing specifications.
460	This is the functional interface between the Cab Radio Adapter, if it exists or the Cab Radio and the OCORA software. It enables the “new generation” Cab Radio to access functions over the UVCCB provided by the MCG for FRMCS connectivity, the JRU for recordings, the DMI (used as HMI for the Cab Radio) and the PIS (connected to the UVCCB through IF495) for passenger announcements or intercom with the train personnel. UIC / TOBA is currently working on this topic.
480	This is the functional interface between the Mobile Communication Gateway (MCG) and the OCORA software. It provides access to the connectivity functions (GSM-R, public radio and FRMCS) implemented on the Mobile Communication Gateway. UIC / TOBA is currently working on this topic.
490	This is the functional interface between the Functional Vehicle Adapter (FVA) (refer to chapter 4.5.1) and the OCORA software. OCORA aims at standardizing this interface.
492	This is the functional interface between the Train Integrity Adapter (TIA) (refer to chapter 4.5.2) and the OCORA software. OCORA aims at standardizing this interface.
495	This is the functional interface between the Functional Passenger Information System Adapter (FPIA) (refer to chapter 4.5.3) and the OCORA software. OCORA aims at standardizing this interface.
RCA-5	This interface is identical to interface RCA-5 assigned to the “CCS On-Board” scope.
RCA-6	This interface is identical to interface RCA-6 assigned to the “CCS On-Board” scope.
RCA-8	This interface is identical to interface RCA-8 assigned to the “CCS On-Board” scope.
508	This interface is identical to interface RCA-8 assigned to the “CCS On-Board” scope.
RCA-41	This interface is identical to interface RCA-41 assigned to the “CCS On-Board” scope.
541	This interface is identical to interface 541 assigned to the “CCS On-Board” scope.
RCA-42	This interface is identical to interface RCA-42 assigned to the “CCS On-Board” scope.

Interface ID	High-Level Description
542	This interface is identical to interface 542 assigned to the “CCS On-Board” scope.
RCA-43	This interface is identical to interface RCA-43 assigned to the “CCS On-Board” scope.
543	This interface is identical to interface 543 assigned to the “CCS On-Board” scope.
SFERA	This interface is identical to interface SFERA assigned to the “CCS On-Board” scope.

Table 14 External functional IFs of the “OCORA Core” scope (OSI Layer 7)

7 Computing platform

7.1 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.

7.2 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 [5], [6], and Appendix A.

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.

7.3 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 MCG and the OCORA Gateway).

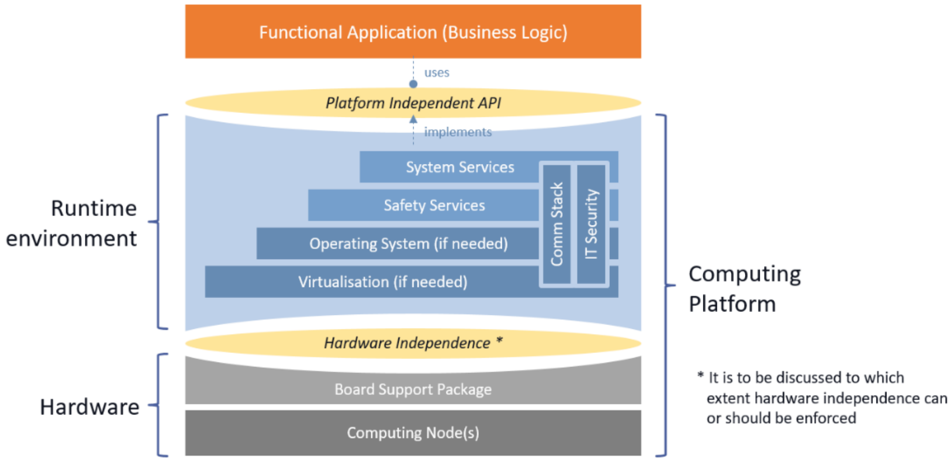

Figure 12 Creating hardware independence

7.3.1 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 Universal Vital Control & Command bus, 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 OCORA gateway).

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.

7.3.2 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 on the Universal Vital Control & Command bus provides standardised access to peripheral devices and external systems (via the OCORA gateway). 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 shall support and maintain computing-node hardware modules of at least two independent hardware manufactures during the entire lifetime of the computing platform.

7.4 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 MCG and the OCORA Gateway)
- **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 shows three possible options on how the internals of the computing platform could look like. The presented options are intended to illustrate the idea only.

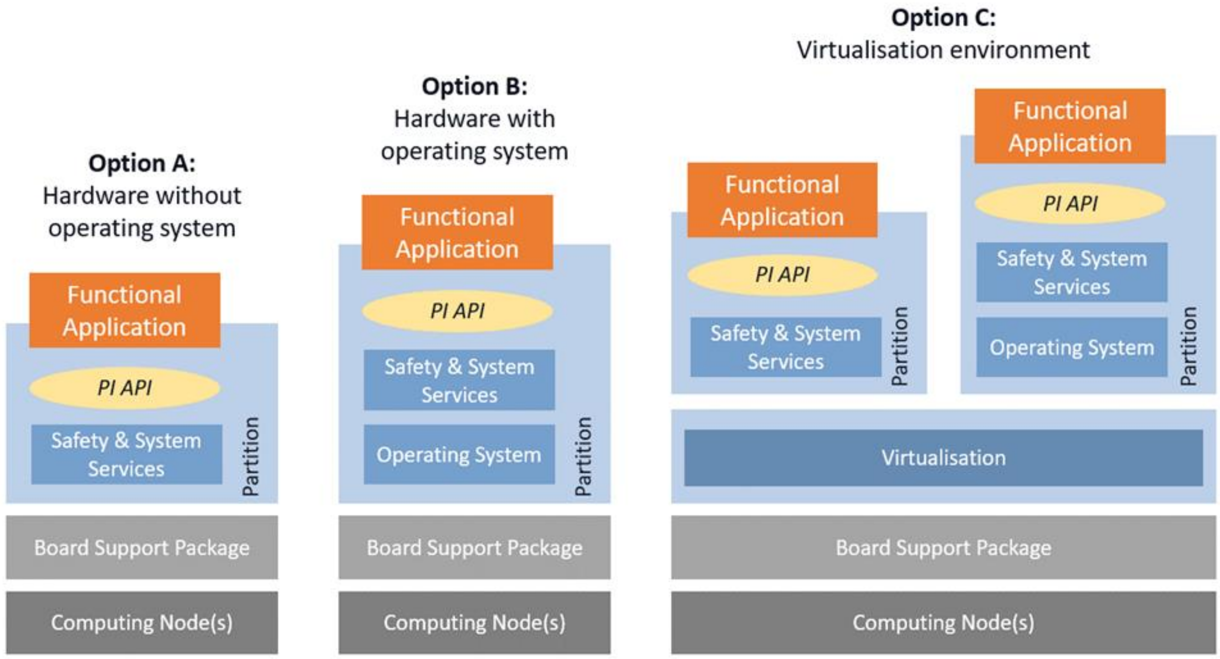

Figure 13 Platform approaches

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.

Option A: The computing platform is implemented on fully embedded hardware, using a board support package and no Operating System. Such a platform could be composed of multiple similar computing-nodes.

Option B: The computing platform uses hardware, board support package and some operating system. Again, such a platform could comprise several computing-nodes.

Option C: The computing platform uses a virtualization environment that allows running multiple partitions on the same hardware. Partitions are execution environments that may contain their own operating system. If required, such a platform could also make use of several computing-nodes using virtualization.

All afore mentioned options shall be considered as a non-exhaustive list of possible platform approaches. A joint OCORA/RCA initiative 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 [10] and a set of high level requirements [15] that shall help industry discussions with the goals 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.

8 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 the Gamma 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.

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

Further information on cyber security is published in document [8] and [14]. 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 System architecture guidelines

A1 Prerequisites for system decomposition

The overall goals of the system decomposition are to enable:

1. “Plug & play”-like exchangeability of CCS building blocks, i.e. (software) applications to be updated, upgraded, removed, added, or exchanged without the need for hardware changes or (re)certification of other than the (software) application affected.
2. Fast, simple and – whenever feasible from a point of view of system performance, cyber security, and operational effort – remote replacement, update, or upgrade of software.
3. Simplified and – where possible – automated safety case development and certification; component oriented (modular) certification.
4. Compatibility alignment on application level between CCS on-board building blocks and between train borne and trackside.
5. Modular testing, acceptance, and certification.

A2 Decomposition principles and rules

The decomposition of the CCS on-board in single building blocks is a key task and needs to be achieved according to a set of decomposition rules and principles that follow the OCORA design principles listed in document [5].

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".

Top level requirements for decomposing the on-board CCS are:

1. Decomposition shall be based on the lowest reasonable granularity to enable the maximum level of value for money. Building blocks shall have narrow interfaces (low coupling) and must allow for regression free testing.
2. Since the function requiring the highest safety integrity level defines the safety integrity level required of all other functions in the same application or service, mixing of functions requiring different safety integrity levels in one application or service shall be prevented.
3. CCS on-board functions not needed in the future (e.g. GSM-R), shall be isolated. This allows easy removal, once the functionality is not needed anymore.
4. Single building blocks are strictly isolated and connected by testable FFFIS.
5. It is considered that physical distribution of building blocks / components over the train is needed in some cases (e.g. antenna positioning, etc.)
6. Functionality not needed in all CCS on-board implementations are isolated in separate building blocks or components, allowing to deploy functionality on an as needed basis.
7. Strategy for product selection (e.g. off the shelf products, make or buy, RU's IT strategy, procurement strategy, different or multiple suppliers, etc.) is considered.
8. Coherence and consistency of life-cycle management on a building block level must be achieved. This is to achieve an independent life-cycle management for each of the building blocks. CCS on-board functions which are identified as likely to evolve in the future or which have often evolved during the

previous baselines (e.g. ATO, localisation, CR about re-localisation (CR782, CR1370), braking curves) shall be isolated in a separate building block or component.

A3 Business decomposition guidelines

Modularity required due to different life cycles

The railway sector is challenged with long asset life cycles conflicting with the introduction of consumer-based technologies. The asset life cycles on absolute level are decreasing, but relevant and identified as first driver for modularity are different, none-overlapping life cycles.

- Rolling Stock asset life cycle (ex. 20-40 years)
- CCS On-board life cycle (ex. 10-15 years)
- Connectivity technology life cycle (ex. 2-5 years)

Modularity required due to adaptation

Within the life cycle of a CCS On-board system the solution might need to be adapted. Typical cases are:

- Non-safe modifications (ex. Cyber-Security patching)
- Safety relevant modifications (ex. Error correction)
- Upgrades (ex. new Baseline)

Modularity required due to introduction of new functionality

The architectural framework of OCORA need to foresee a way of serving additional business needs. Within the life cycle of a CCS On-board system new functionality might be introduced. This could require:

- Additional peripherals (ex. sensors for automation)
- Additional applications (ex. new functionality)

Minimum modularity from a business perspective

As a summary the following aspects need to be transparently available:

1. Interface between VCS / PIS and CCS On-board
2. Interface between CCS On-board and Connectivity
3. UVCCB, OSI 1-7 (new peripherals)
4. API (new applications)
5. The modularity for system adaptation needs to be solved contractually with the related OEM for the respective building blocks.

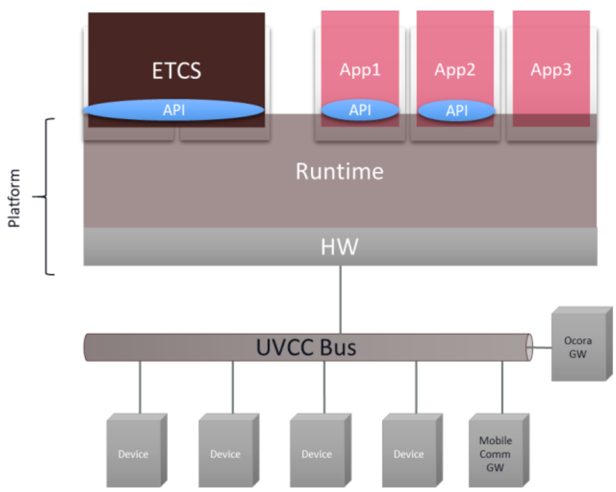

Figure 14 Minimal Modularity

A4 Architecture design guidelines

The OCORA architecture design principles formulated in document [5] can be operationalised in to the system architecture design guidelines that are applied in this document.

System architecture design guidelines	OCORA architecture design principles						
	openness	modularity	exchangeability	migrateability	evolvability	portability	security
1. The CCS on-board shall be decomposed according to the rules defined in Appendix A1 - A3.	x	x	x	x	x	x	
2. Functions shall be realised in software (applications and services) and should not be bound to a specific hardware.	x	x	x	x	x	x	
3. System design shall enable software to be updated, upgraded, removed, added, or exchanged without the need for hardware changes or (re)certification of other than the software affected. Means to ensure backward compatibility must be provided.	x	x	x	x	x	x	x
4. Core ETCS functionality shall be isolated from other on-board functions and the core ETCS functionality shall be decomposed according to the rules defined in Appendix A1 - A3.	x	x	x	x	x	x	
5. CCS on-board functionality foreseeable to become obsolete in the future shall be isolated to ensure easy decommissioning, once the respective functionality is not needed anymore.	x	x	x	x	x	x	
6. Whilst and where no standardized and common CCS-VCS-PIS network/bus is available, the CCS on board shall communicate with vehicle functions through a gateway.	x	x	x	x	x	x	x
7. Open standards are used wherever possible and reasonable.	x	x	x	x	x	x	x
8. The re-use of software is maximized (same software for various deployments).	x	x	x	x	x	x	
9. A service-oriented architecture on application level shall avoid duplication of code. Therefore, common applications or application services will be identified.	x	x	x	x	x	x	
10. The architecture/design provides support for automated testing.		x	x	x	x	x	
11. The on-board CCS system is optimized regarding the optimal number of building blocks.	x	x					
12. Hardware is separated from software, allowing to handle the different life cycle profiles.	x	x	x	x	x	x	
13. The architecture considers that a competitive market for the different building blocks can develop.	x	x	x	x	x	x	

Table 15 System architecture design guidelines

Appendix B 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.

B1 Scenario 1a: Legacy train 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 VCS 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 UVCCB, following the OCORA interface standard. Refer to Appendix C for further details.

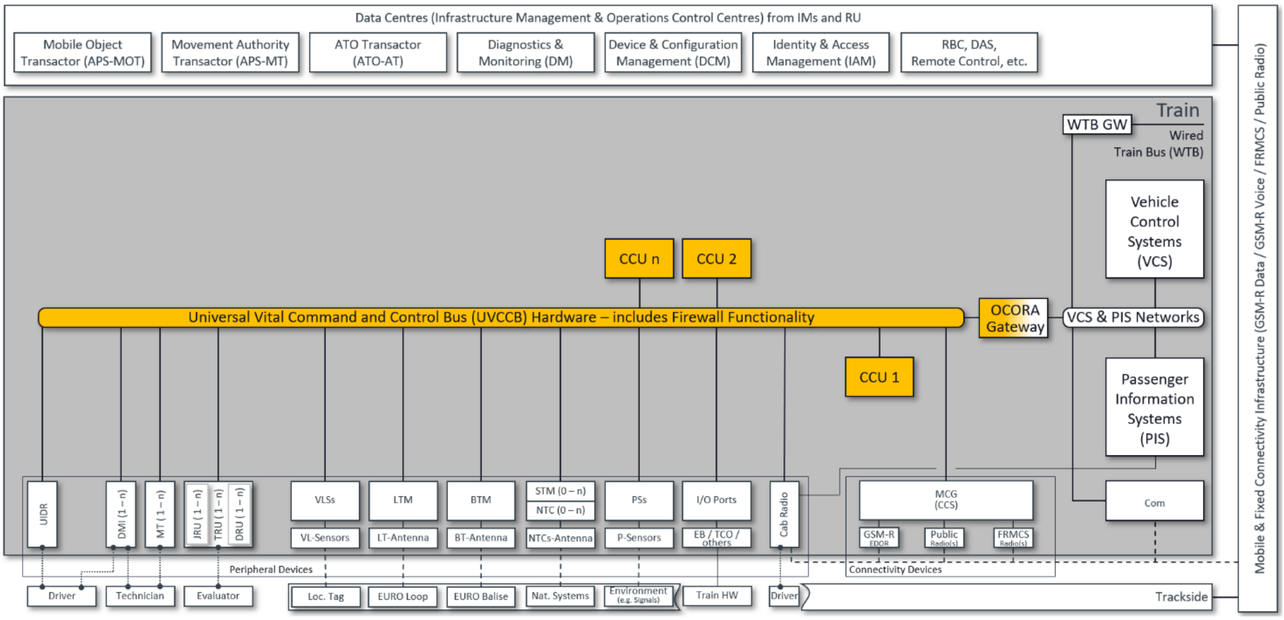

Figure 15 Legacy Train with OCORA Compliant CCS Peripherals

B2 Scenario 1b: Legacy train with legacy peripherals using adapters

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 VCS is implemented through the OCORA Gateway and the respective Functional Vehicle Adapter (FVA). This scenario further assumes that legacy Peripheral Devices are connected though an adapter (see red boxes) to the UVCCB, following the OCORA interface standard.

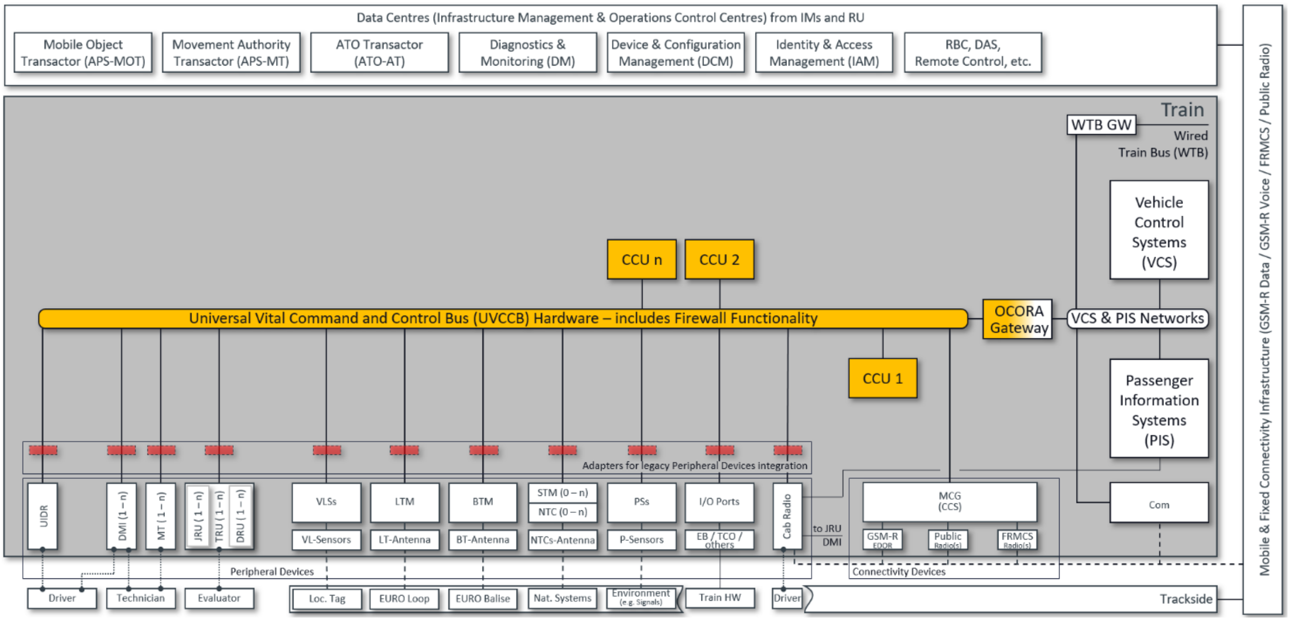

Figure 16 Legacy Train with Legacy CCS Peripherals connected with Adapters

B3 Scenario 1c: Legacy train with legacy peripherals w/o adapters

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 VCS is implemented through the OCORA Gateway and the respective Functional Vehicle Adapter (FVA). This scenario further assumes that some (or all) Peripheral Devices are not connected via the UVCCB, e.g. GSM-R EDOR, STM (refer to red connections), etc.

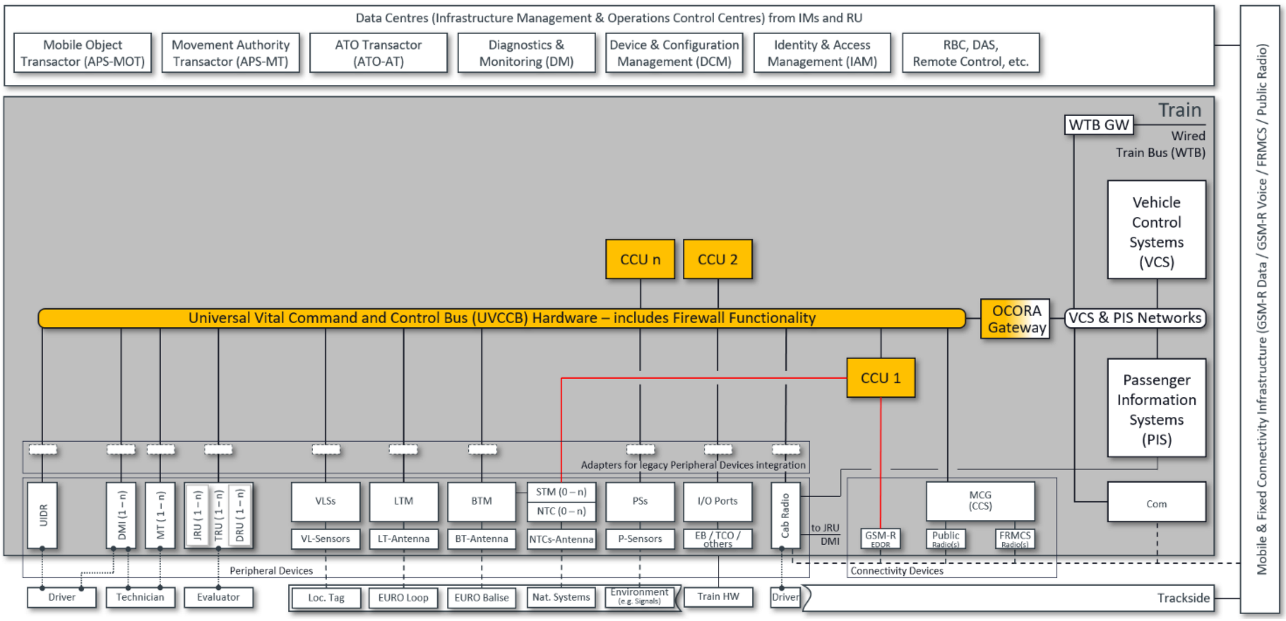

Figure 17 Legacy Train with Legacy CCS Peripherals w/o Adapters

B4 Scenario 2: NG-TCN Train – Separate networks

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The CCS Network and the NG-TCN network are separate networks and the communication with the VCS is implemented through an ECN/ECN Gateway. This scenario further assumes that all Peripheral Devices and Connectivity Devices are OCORA compliant and are therefore directly connected to the UVCCB, following the OCORA interface standard. Refer to Appendix C for further details.

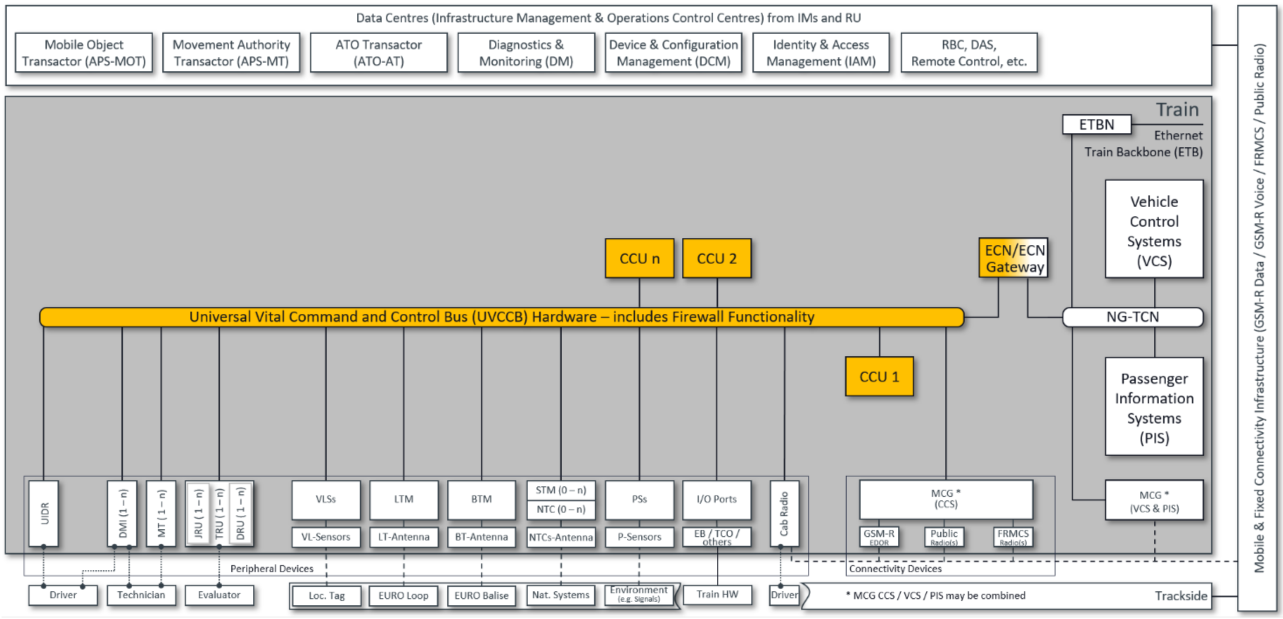

Figure 18 NG-TCN Train – Separate Networks

B5 Scenario 3: NG-TCN Train – Common network

This scenario applies to all cases where an OCORA compliant CCS System is integrated into a Train having a NG-TCN. The CCS Network and the NG-TCN network are combined (different virtual networks) and the communication with the VCS is implemented through an ECN/ECN Gateway. This scenario further assumes that all Peripheral Devices and Connectivity Devices are OCORA compliant and are therefore directly connected to the UVCCB, following the OCORA interface standard. Refer to Appendix C for further details.

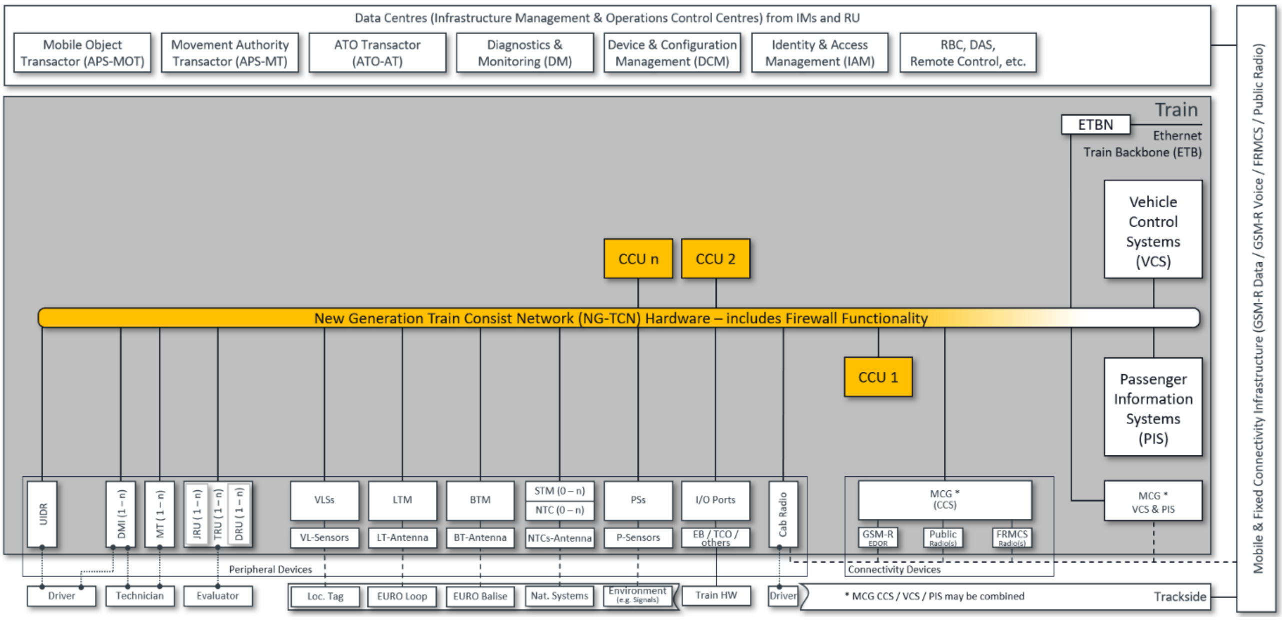

Figure 19 NG-TCN Train – Common Network

Appendix C 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 and to connect and integrate the connectivity devices. These scenarios are the basis for further discussions about connectivity and the OCORA Gateway (OCORA-GW) and will be adapted as the architecture evolves.

C1 Scenario 1 – Legacy Train / MCG connected to UVCCB

This scenario covers the integration of an OCORA compliant CCS on-board system into an existing vehicle equipped with a legacy Vehicle Control System (VCS) and/or Passenger Information Systems (PIS). Trackside connectivity for the CCS on-board is provided by the MCG connected to the UVCCB (CCS-ECN).

The integration between CCS on-board and Vehicle Networks (VCS and PIS) is always vehicle specific and the adaptations (Layer 1 to 7) are implemented on the OCORA-GW. Trackside connectivity (indicated as "Com" in Figure 20) for the Vehicle Networks may already exist and therefore not use the trackside connectivity (MCG) of the CCS Network.

Figure 20 provides the topology view whereas Figure 21 provides a logical view regarding the trackside connectivity and cyber security aspects.

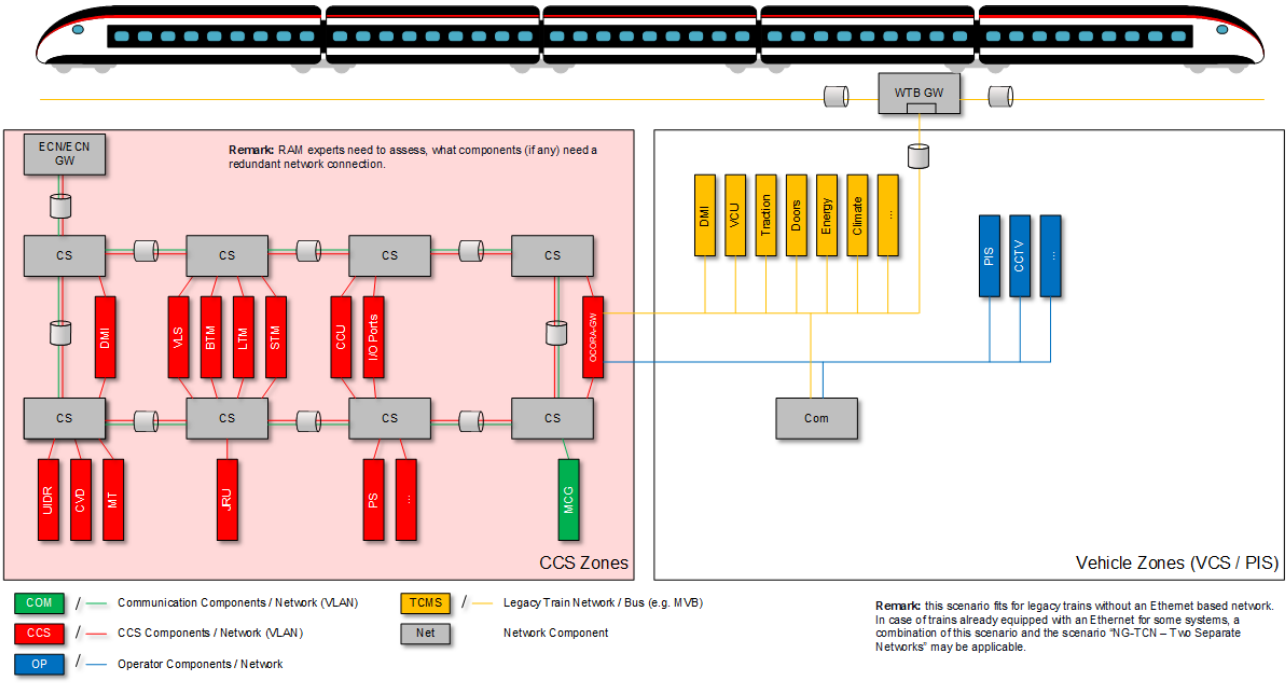

Figure 20 Network Topology of scenario 1 – Legacy Train / MCG connected to UVCCB

This is the most appropriate scenario for integrating an OCOCRA compliant CCS on-board system into a legacy train.

Cyber-security between trackside and onboard networks and between the onboard networks is implemented at different areas within the onboard system. The table below provides an overview, where cyber-security aspects are covered for the different transition points.

Transition point	Cyber-security aspects covered in:	Remark
UVCCB <-> Trackside	Mobile Communication Gateway (MCG)	
Legacy-TCN <-> Trackside	N/A	If the Legacy-TCN (VCS- /PIS-Network) has its own trackside connectivity
Legacy-TCN <-> UVCCB	(OCORA-GW)	The OCORA-GW implements the required protocol adaptations to integrate the Vehicle Control System (VCS) and the Passenger Information System (PIS) with the CCS on-board. There is no direct physical link between the CCS on-board and the VCS/PIS.

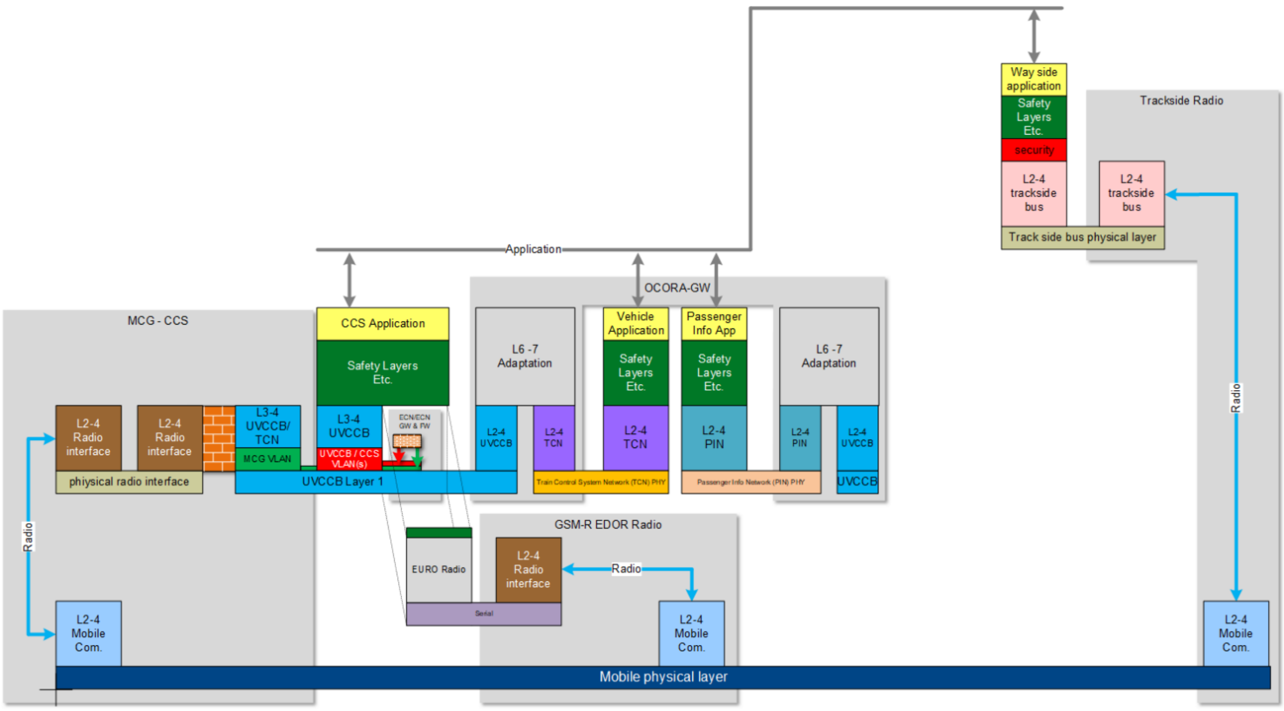

Figure 21 Logical view of scenario 1 – Legacy Train / MCG connected to UVCCB

C2 Scenario 2 – Separate Networks / MCG connected to UVCCB

In this scenario, the CCS Network (UVCCB) and the on-board networks (Train Control Network and Passenger Information Network) are physically separated. The Mobile Communication Gateway is connected to the CCS Network providing cybersafe trackside connectivity for the CCS on-board, VCS and PIS networks.

The central element between the onboard networks is the ECN/ECN GW. The ECN/ECN GW routes the traffic between the onboard networks and acts as firewall between them.

Figure 22 provides the topology view whereas Figure 23 provides a logical view regarding the trackside connectivity and cyber security aspects.

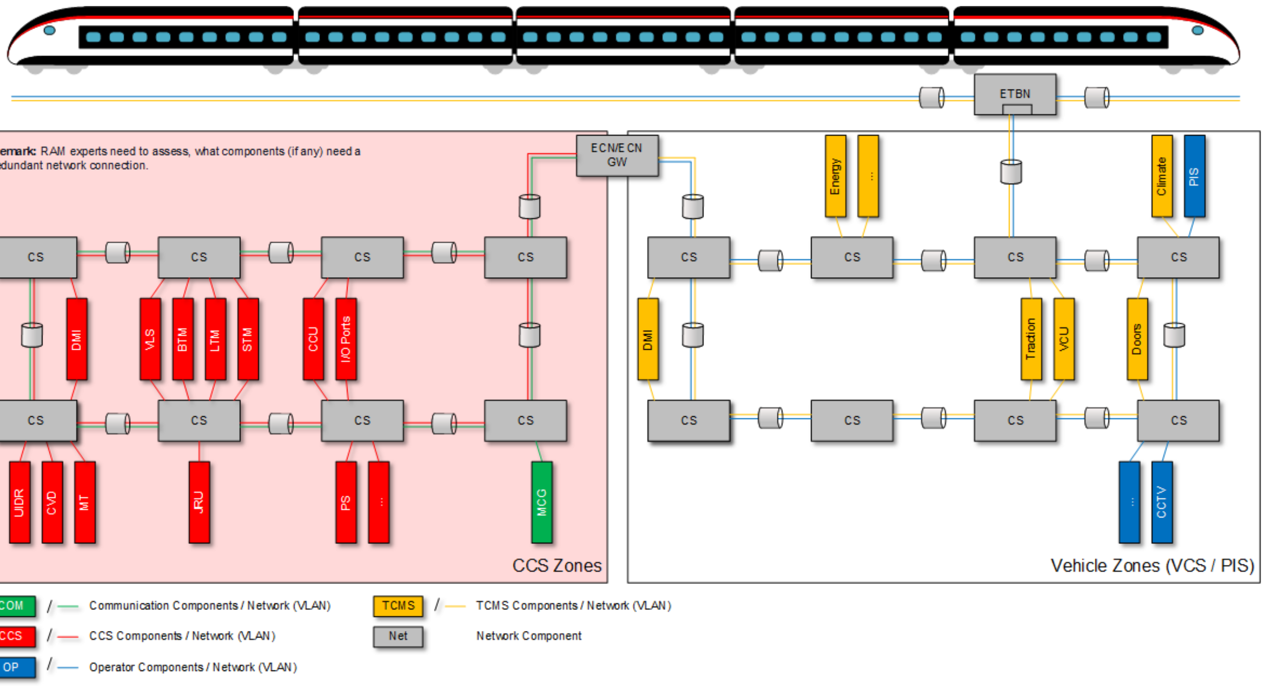

Figure 22 Network Topology of scenario 2 – Separate Networks / MCG connected to UVCCB

Cyber-security between trackside and onboard networks and between the onboard networks is implemented at different areas within the onboard system. The table below provides an overview, where cyber-security aspects are covered for the different transition points.

Transition point	Cyber-security aspects covered in:	Remark
UVCCB <-> Trackside	MCG-CCS	
UVCCB <-> UVCCB	ECN/ECN GW	Between CCS-VLAN and MCG-VLAN (connectivity VLAN)
NG-TCN <-> Trackside	ECN/ECN GW & MCG-CCS	
NG-TCN <-> UVCCB	ECN/ECN GW	
NG-TCN <-> NG-TCN	ECN/ECN GW	Between Train VLANS (VCS-VLAN and PIS-VLAN)

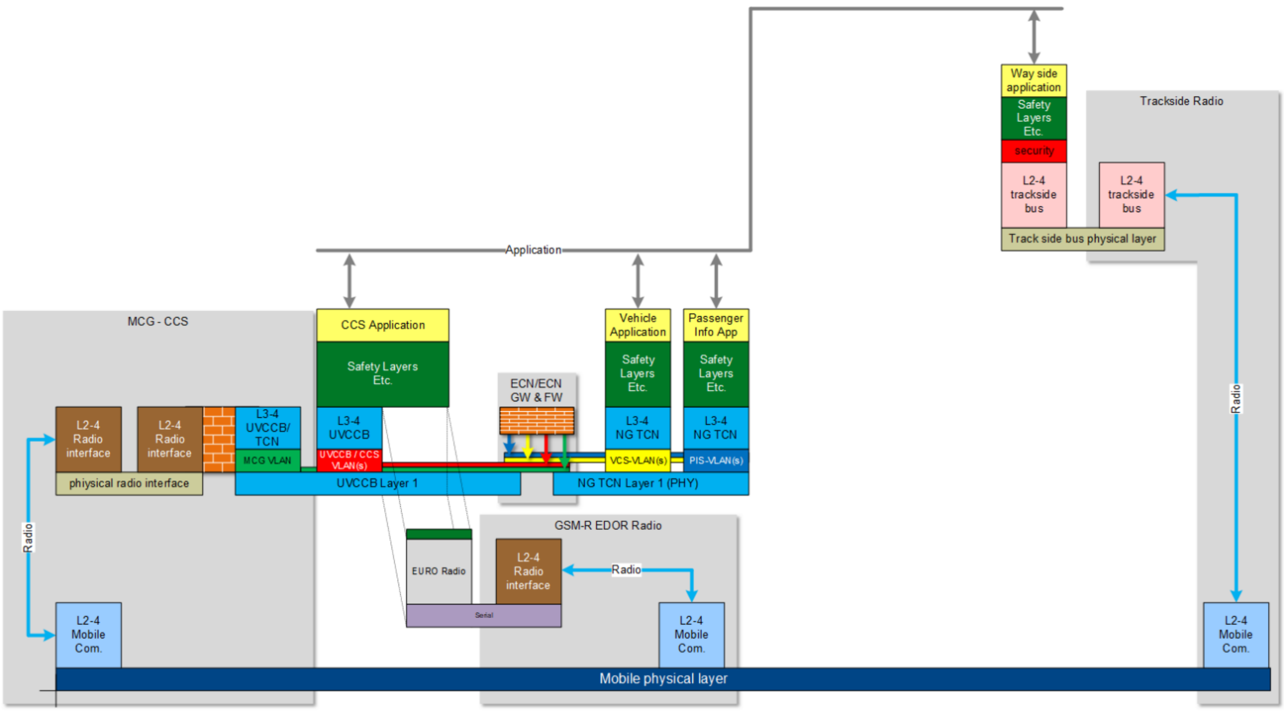

Figure 23 Logical view of scenario 2 – Separate Networks / MCG connected to UVCCB

The table below provides an initial evaluation of this scenario against the OCORA Architecture Design Principles where applicable. This evaluation will be discussed in more detail in the upcoming OCORA releases.

Criteria	Advantages	Disadvantages
Openness		
Modularity		
Exchangeability		
Migrateability		
Evolvability		▪ Functional updates to the VCS or PIS may imply also updates to the MCG connected to the CCS Network and the CCS global safety demonstration.
Portability		
Security	▪ One single potential entry point from trackside to the onboard networks ▪ The MCG-CCS will have a cyber level aligned with the CCS cyber requirements ▪ Physical segregation between CCS Network and Train Network	
Reliability		▪ Synchronisation between the two separate onboard networks to assure deterministic communication may be difficult or cause jitter.
Availability		▪ Will a shared MCG be able to address trackside on different telecom media with possibly different levels of availability and cyber security requirements?
Maintainability	▪ One single MCG to be maintained in a safe condition	
Safety		
Economical Aspects	▪ One single MCG, therefore less costs for the trackside connectivity	▪ Additional costs due to the two separate networks (e.g. additional consist switches)

Table 16 Evaluation scenario 2 – Separate Networks / MCG connected to UVCCB

C3 Scenario 2a – Separate Networks / MCG connected to TCN

In this scenario, the CCS Network (UVCCB) and the on-board networks (Train Control Network and Passenger Information Network) are physically separated. The Mobile Communication Gateway is connected to the Train Network providing cybersafe trackside connectivity for the onboard VCS, PIS and CCS networks.

The central element between the onboard networks is the ECN/ECN GW. The ECN/ECN GW routes the traffic between the onboard networks and acts as firewall between them.

Figure 24 provides the topology view whereas Figure 25 provides a logical view in regard to the trackside connectivity and cyber security aspects.

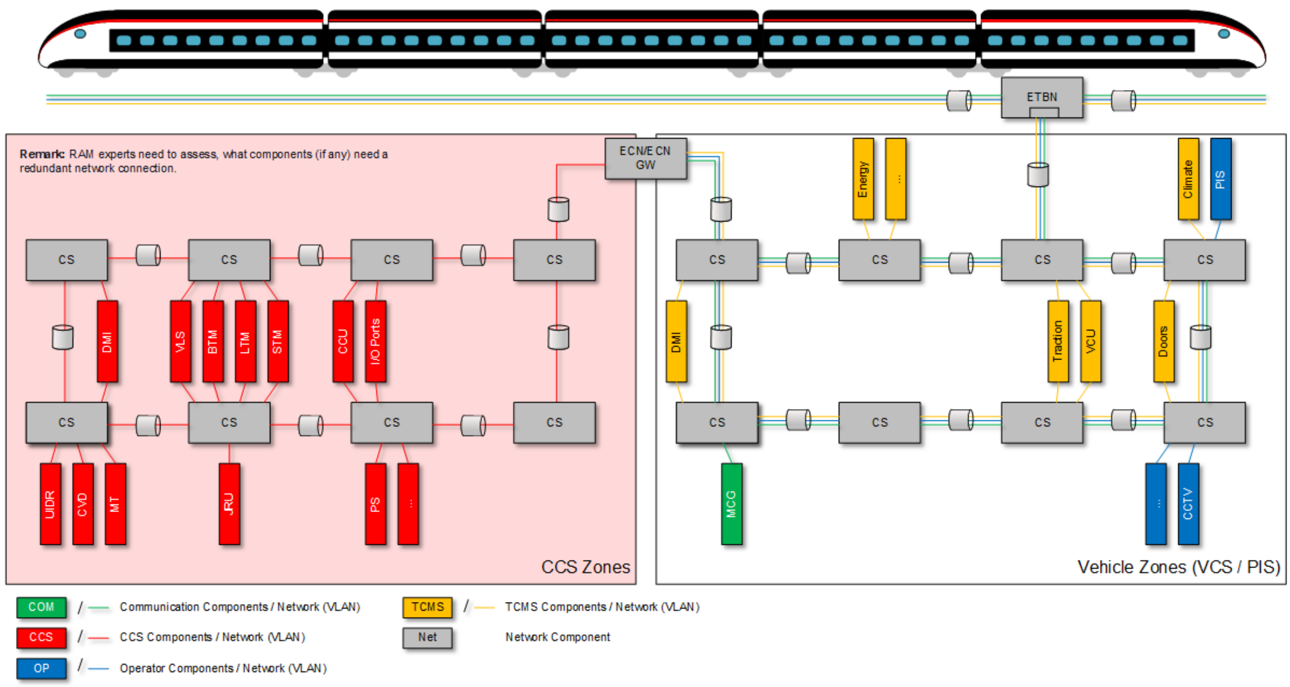

Figure 24 Network Topology view of scenario 2a – Separate Networks / MCG connected to TCN

Cyber-security between trackside and onboard networks and between the onboard networks is implemented at different areas within the onboard system. The table below provides an overview, where cyber-security aspects are covered for the different transition points.

Transition point	Cyber-security aspects covered in:	Remark
UVCCB <-> Trackside	MCG-TCN	
UVCCB <-> UVCCB	ECN/ECN GW	Between CCS-VLAN(s)
NG-TCN <-> Trackside	ECN/ECN GW & MCG-TCN	
NG-TCN <-> UVCCB	ECN/ECN GW	
NG-TCN <-> NG-TCN	ECN/ECN GW	Between Train VLANS (VCS-VLAN and PIS-VLAN)

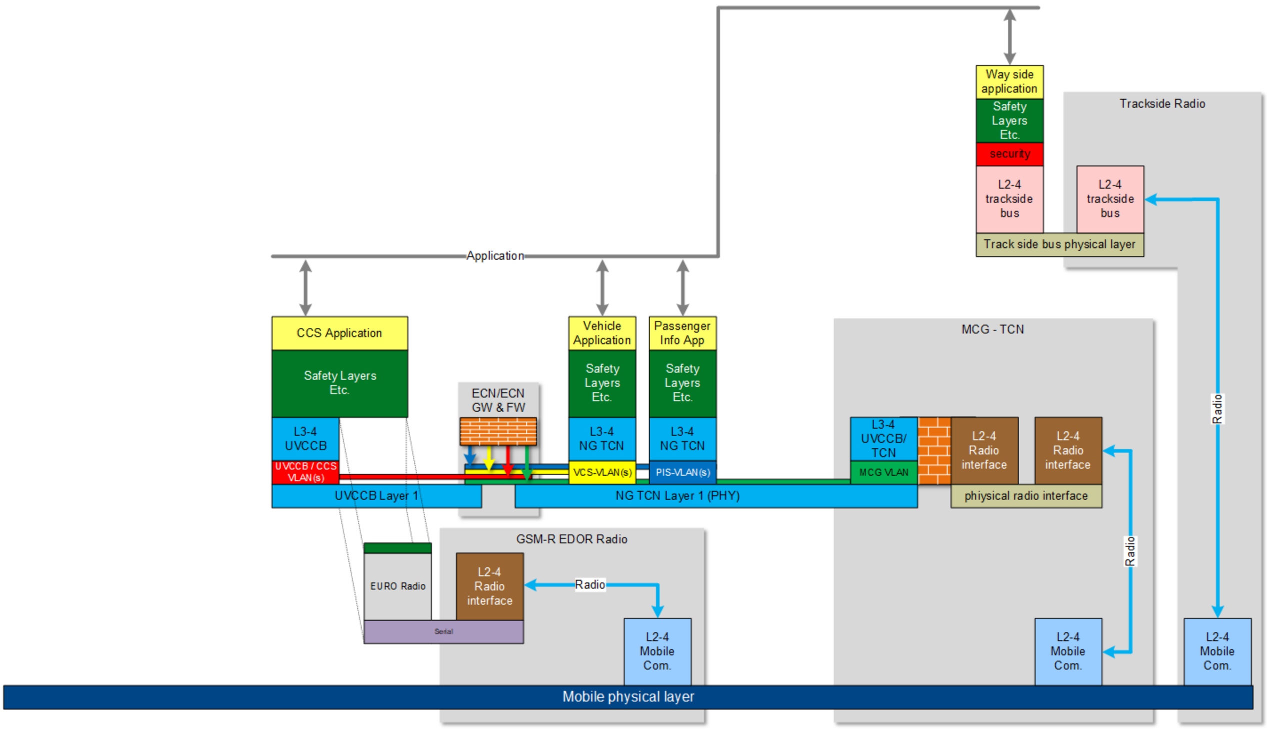

Figure 25 Logical view of scenario 2a – Separate Networks / MCG connected to TCN

The table below provides an initial evaluation of this scenario against the OCORA Architecture Design Principles where applicable. This evaluation will be discussed in more detail in the upcoming OCORA releases.

Criteria	Advantages	Disadvantages
Openness		
Modularity		
Exchangeability		
Migrateability		
Evolvability		▪ Impact of the telecom life-cycle / TCN functional needs on the MCG-TCN carrying the CCS connectivity to the CCS global safety demonstration.
Portability		
Security	▪ One single potential entry point from trackside to the onboard networks ▪ Physical segregation between CCS Network and Train Network	▪ The MCG-TCN will have a cyber level aligned with the TCN cyber requirements which may not fulfil the CCS on-board requirements.
Reliability		▪ Synchronisation between the two separate onboard networks to assure deterministic communication may be difficult or cause jitter.
Availability		▪ Will a shared MCG be able to address trackside on different telecom media with possibly different levels of availability and cyber security requirements?
Maintainability	▪ One single MCG to be maintained in a safe condition	
Safety		
Economical Aspects	▪ One single MCG, therefore less costs for the trackside connectivity	▪ Additional costs due to the two separate networks (e.g. additional consist switches)

Table 17 Evaluation scenario 2a – Separate Networks / MCG connected to TCN

C4 Scenario 2b – Separate Networks / MCG on both Networks

In this scenario, the CCS Network (UVCCB) and the on-board networks (Train Control Network and Passenger Information Network) are physically separated. There is a dedicated Mobile Communication Gateway connected to each of the onboard Networks providing cybersafe trackside connectivity for the onboard VCS, PIS and CCS networks.

The central element between the onboard networks is the ECN/ECN GW. The ECN/ECN GW routes the traffic between the onboard networks and acts as firewall between them.

Figure 26 provides the topology view whereas Figure 27 provides a logical view in regard to the trackside connectivity and cyber security aspects.

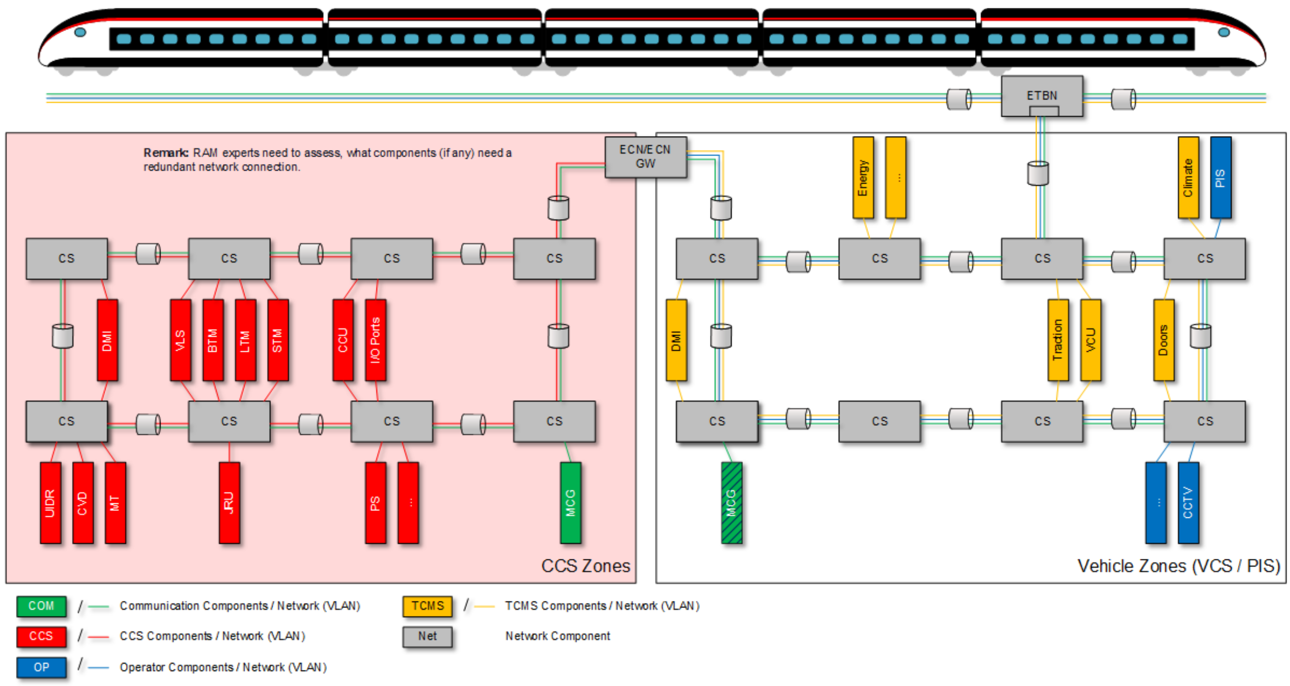

Figure 26 Network Topology of scenario 2b – Separate Networks / MCG on both Networks

Cyber-security between trackside and onboard networks and between the onboard networks is implemented at different areas within the onboard system. The table below provides an overview, where cyber-security aspects are covered for the different transition points.

Transition point	Cyber-security aspects covered in:	Remark
UVCCB <-> Trackside	MCG-CCS	
UVCCB <-> UVCCB	ECN/ECN GW	Between CCS-VLAN(s)
NG-TCN <-> Trackside	MCG-TCN	
NG-TCN <-> UVCCB	ECN/ECN GW	
NG-TCN <-> NG-TCN	ECN/ECN GW	Between Train VLANS (VCS-VLAN and PIS-VLAN)

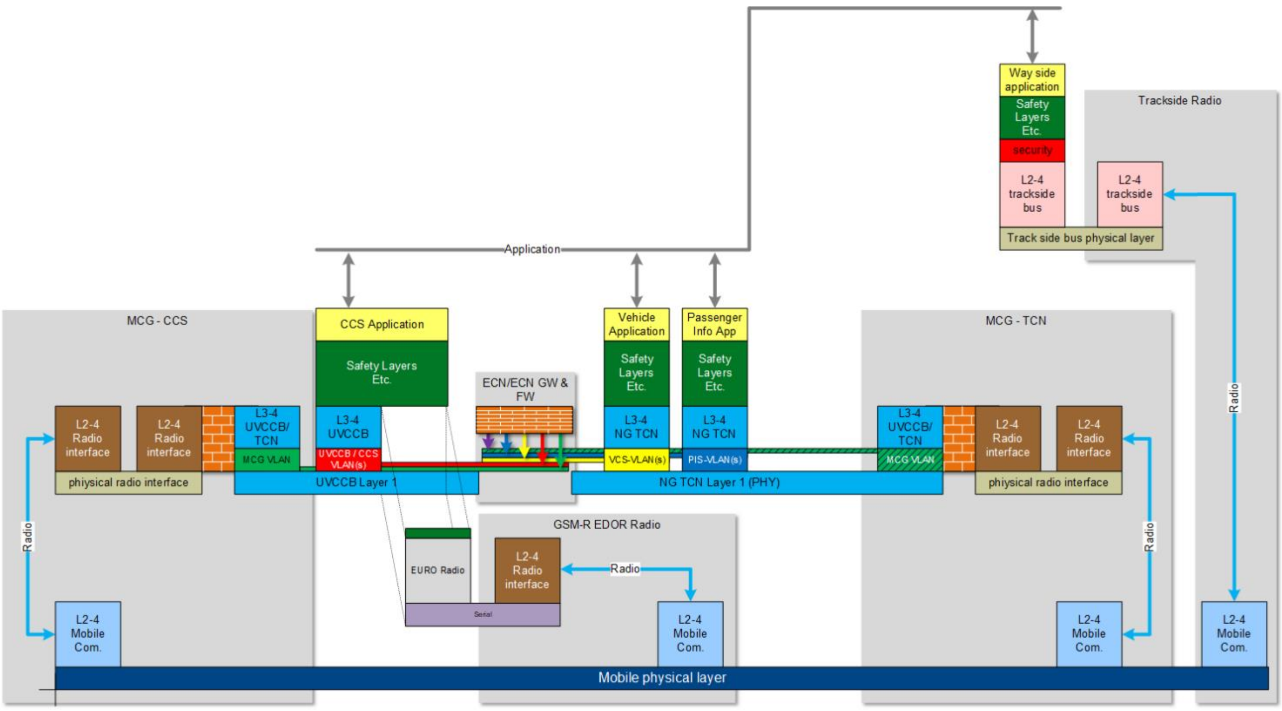

Figure 27 Logical view of scenario 2b – Separate Networks / MCG on both Networks

The table below provides an initial evaluation of this scenario against the OCORA Architecture Design Principles where applicable. This evaluation will be discussed in more detail in the upcoming OCORA releases.

Criteria	Advantages	Disadvantages
Openness		
Modularity		
Exchangeability		
Migrateability		
Evolvability	▪ Limiting the impacts that a functional change in one area (CCS, VCS or PIS) could have on the MCG connected to the of the other areas network. ▪ The MCG Life Cycle can more easily follow the life cycle and safety demonstration cycle of each zone (e.g. the MCG on the CCS on-board can stay on a product for a long time, where a MCG on the TCN can more quickly evolve on higher throughput technology without impacting the CCS on-board safety).	▪
Portability		
Security	▪ Each MCG addresses the cyber requirements in proportion to the needs of the connected onboard network. ▪ Physical segregation between CCS Network and Train Network	▪ Two potential entry points from trackside to the onboard networks
Reliability	▪ Separate trackside connectivity reduces potential negative impacts between the onboard networks	
Availability	▪ Separate trackside connectivity improves the availability of the connectivity for each zone (CCS, VCS and PIS)	
Maintainability		▪ More devices (consist switches and 2 MCGs) and therefore higher maintenance
Safety		
Economical Aspects		▪ Additional costs due to the two separate networks (e.g. additional consist switches) ▪ Additional costs due to the use of 2 MCGs

Table 18 Evaluation scenario 2b – Separate Networks / MCG on both Networks

C5 Scenario 3 – Common Network / MCG on common Network

In this scenario the CCS Network (UVCCB) and the Train Network are on the same physical network and all communication to the trackside systems is handled by the Mobile Communication Gateway (MCG) connected to the common NG-TCN.

The central element between the onboard networks is the ECN/ECN GW. The ECN/ECN GW routes the traffic between the VLANs and acts as firewall between them.

Figure 28 provides the topology view whereas Figure 29 provides a logical view in regard to the trackside connectivity and cyber security aspects.

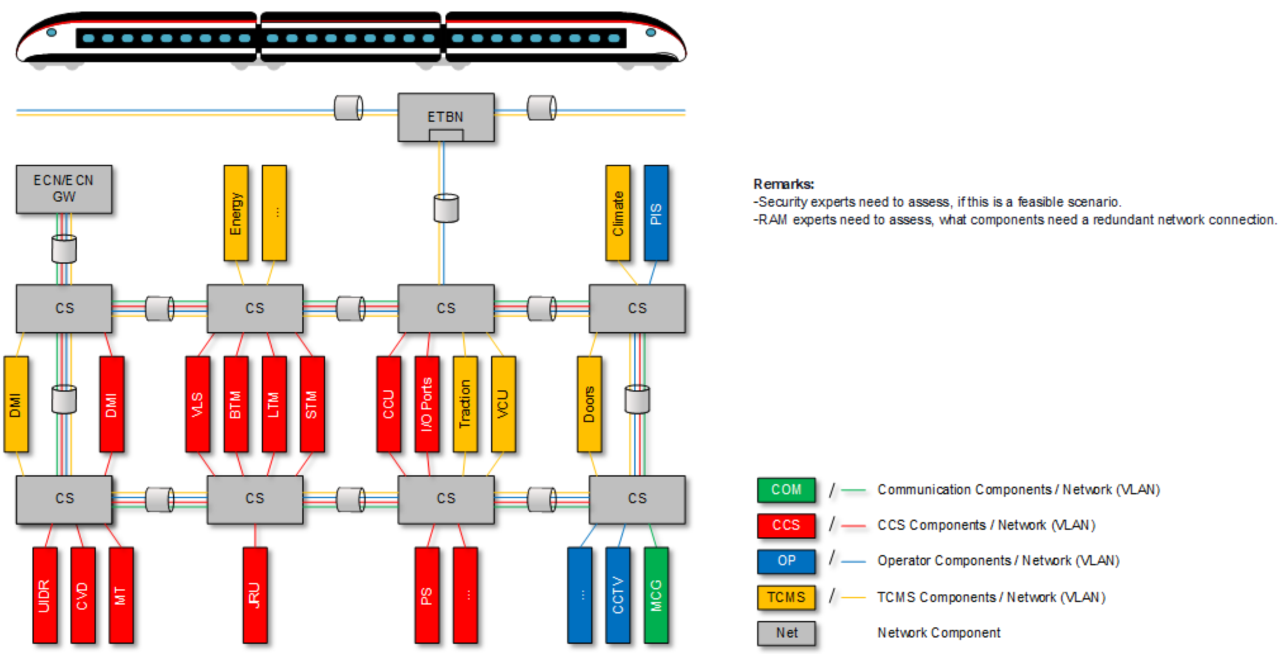

Figure 28 Network Topology of scenario 3 – Common Network / MCG on common Network

Cyber-security between trackside and onboard networks and between the onboard networks is implemented at different areas within the onboard system. The table below provides an overview, where cyber-security aspects are covered for the different transition points.

Transition point	Cyber-security aspects covered in:	Remark
UVCCB <-> Trackside	MCG-CCS	
UVCCB <-> UVCCB	ECN/ECN GW	Between CCS-, VCS- and PIS-VLAN(s)
NG-TCN <-> Trackside	ECN/ECN GW & MCG-CCS	
NG-TCN <-> UVCCB	ECN/ECN GW	
NG-TCN <-> NG-TCN	ECN/ECN GW	Between Train VLANS (VCS-VLAN and PIS-VLAN)

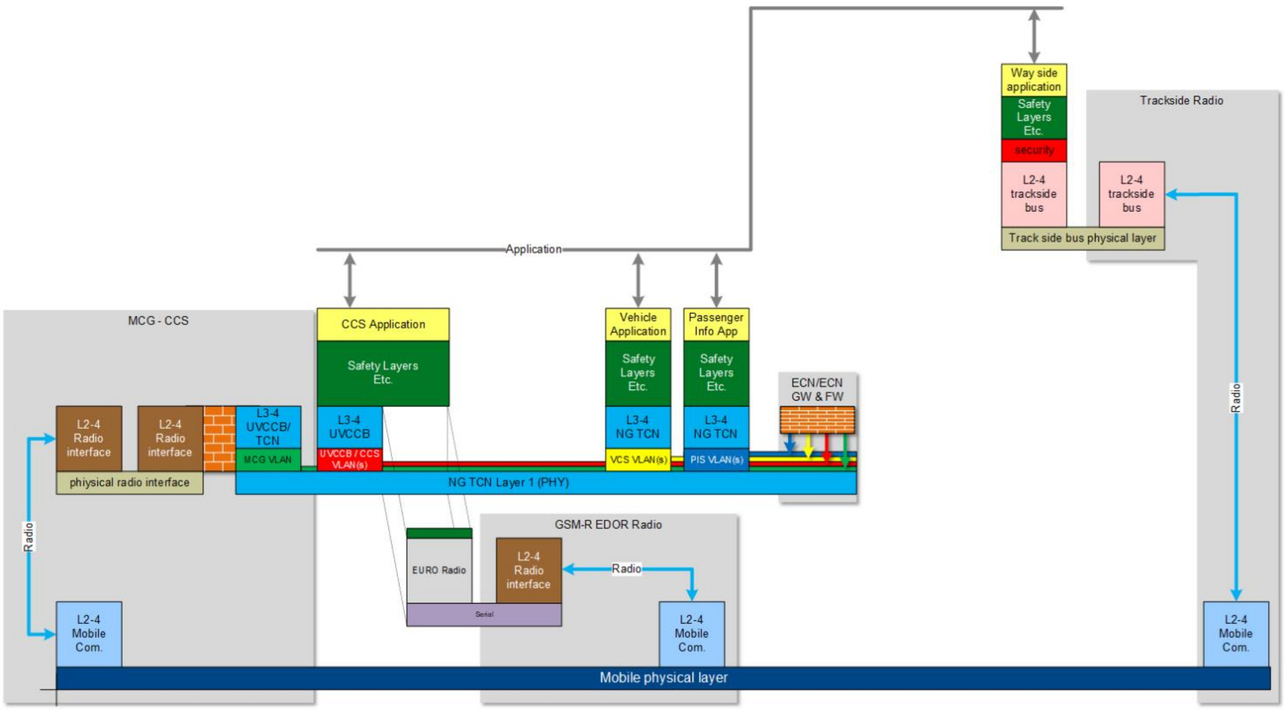

Figure 29 Logical view of scenario 3 – Common Network / MCG on common Network

The table below provides an initial evaluation of this scenario against the OCORA Architecture Design Principles where applicable. This evaluation will be discussed in more detail in the upcoming OCORA releases.

Criteria	Advantages	Disadvantages
Openness		
Modularity		
Exchangeability		
Migrateability		
Evolvability		▪ Functional updates to the VCS or PIS may imply also updates to the MCG connected to the common Network and the CCS on-board global safety demonstration.
Portability		
Security	▪ One single potential entry point from trackside to the onboard networks	▪ No physical segregation between CCS Network and Train Network (segregation on Layer2 through VLANs) ▪ The common MCG will have to fulfil the cyber level aligned with the CCS on-board cyber requirements ▪ Impact on the level of protection of physical access to the network, which would be potentially less on the TCN side (cables crossing the traveller zone) compared to the UVCCB, which may remain confined to a technical zone or cabinet.
Reliability	▪ No potential synchronisation issues for deterministic communication between CCS on-board and VCS.	
Availability		▪ Will a shared MCG be able to address trackside on different telecom media with possibly different levels of availability and cyber security requirements?
Maintainability	▪ One single MCG to be maintained in a safe condition	
Safety		
Economical Aspects	▪ One single MCG, therefore less costs for the trackside connectivity ▪ Use or share of existing (NG-TCN) consist switches	▪ The ECN/ENC GW will have to meet the requirements of the CCS on-board, which may impact cost and maintenance of an ECN/ENC GW.

Table 19 Evaluation scenario 3 – Common Network / MCG on common Network

Appendix D 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 identified in the OCORA Alpha release already: VS = Vehicle Supervisor / VL = Vehicle Locator / MLM = Mode & Level Manager / STMC = STM Control.

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 VS, VL, and the MLM / STMC. 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 complete VS, VL, and MLM / STMC model, identifying additional requirement to SUBSET-026, can be expected in subsequent OCORA documentation releases.

On-Board Functions	Reference SUBSET-026	VS	VL	MLM / STMC	Others
Data Consistency					
Check linking consistency	3.16.2.3 3.4.4	X [2]			
Check Balise Group Message Consistency if linking consistency is checked	3.16.2.4.1 3.16.2.4.3	X [2]			
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 [2]			
Check Unlinked Balise Group Message Consistency	3.16.2.5	X [2]			
Check correctness of radio messages	3.16.3.1.1	X			
Check radio sequence	3.16.3.3	X			
Check safe radio connection (only level 2/3)	3.16.3.4	X			
Determine Train Speed and Position					
Determine train position referenced to LRBG	3.6.1 3.6.4		X		
Determine train speed, train acceleration, train standstill	None		X		
Determine Geographical Position	3.6.6	X	X [3]		
Report train position when train reaches standstill	3.6.5.1.4 a)	X [4]			
Report train position when mode changes to...1	3.6.5.1.4 b)	X [4]			
Report train position when train integrity confirmed by driver	3.6.5.1.4 c)	X [4]			
Report train position when loss of train integrity is detected	3.6.5.1.4 d)	X [4]			
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]			
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]			
Report train position when change of level due to trackside order	3.6.5.1.4 g)	X [4]			
Report train position when change of level due to driver request	3.6.5.1.4 g)	X [4]			
Report train position when establishing a session with RBC	3.6.5.1.4 h)	X [4]			
Report train position when a data consistency error is detected (only level 2/3)	3.6.5.1.4 i)	X [4]			
Report train position as requested by RBC...	3.6.5.1.4	X [4]			
... or Report train position at every passage of an LRBG compliant balise group	3.6.5.1.4 j)	X [4]			
Determine Train Speed and Position					
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			
Request MA Cyclically when "Start" is selected (only level 2/3)	4.4.11 5.4, 5.11	X			
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			
Request MA on track description deletion (only level 2/3)	3.8.2.7.3	X			
Determine EOA/LOA, SvL, Danger Point, etc...	3.8.4 3.8.5	X			
Handle Co-operative MA revocation (only level 2/3)	3.8.6	X			
Manage Unconditional Emergency Stop	3.10	X			
Manage Conditional Emergency Stop	3.10	X			
Determine Most Restrictive Speed Profile, based on:					
SSP	3.11.3	X			
ASP	3.11.4	X			
TSR	3.11.5	X			
Signalling related speed restriction when evaluated as a speed limit	3.11.6	X			
Mode related speed restriction	3.11.7	X			
Train related speed restriction	3.11.8	X			

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

On-Board Functions	Reference SUBSET-026	VS	VL	MLM / STMC	Others
STM max speed	3.11.2.2 g)	X			
STM system speed	3.11.2.2 h)	X			
LX speed	3.12.5.6	X			
Speed restriction to ensure a given permitted braking distance	3.11.11	X			
Override related speed restriction	5.8.3.6	X			
Supervise Train Speed					
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			
Speed and Distance Monitoring based on MRSP	4.4.10.1	X			
Speed and Distance Monitoring based on MRSP, allowed distance to run in Staff Resp. mode	4.4.11	X			
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					
Backwards Distance Monitoring	4.4	X			
Roll Away Protection	3.14.2	X			
Reverse Movement Protection	3.14.3	X			
Standstill Supervision	3.14.4 4.4.7.1.5	X			
Supervise “danger for shunting” information and list of expected balises for shunting	4.4.8.1.1 b) and c)	X			
Supervise “Stop if in SR” information and list of expected balises for Staff Responsible	4.4.11.1.3 c) and d)	X			
Supervise signalling related speed restriction when evaluated as a trip order	3.11.6.4	X			
Command Emergency Brake	4	X		tbd	NTC-APPs APV
Determine Mode and Level					
Determine ERTMS/ETCS Mode	3.12.4 4.6	tbd		tbd	
Determine ERTMS/ETCS level	5.10	tbd		tbd	
Other functions					
System Version Management	3.17	X			
Manage Communication Session	3.5	X [5]			
Delete Revoked TSR	3.11.5.5	X			
Override (Trip inhibition)	5.8	X			
Manage Track Conditions excluding Sound Horn, Non-Stopping Areas, Tunnel Stopping Areas and Big Metal Masses	3.12.1	X			
Manage Track Conditions Sound Horn, Non-Stopping Areas, Tunnel Stopping Areas	3.12.1	X			
Manage Track Condition Big Metal Masses	3.12.1	X			
Manage Route Suitability	3.12.2	X			
Manage Text Display to the driver	3.12.3	X			
Manage LSSMA display to the driver	4.4.19.1	X			
Manage RBC/RBC Handover (only level 2/3)	3.15.1 5.15	X [6]			
Manage Track Ahead Free Request (only level 2/3)	3.15.5	X			
Provide Fixed Values, and Default/National Values	3.18.1 3.18.2	X			
Manage change of Train Data from external sources	5.17	X			
Provide Date and Time	3.18.5				TSS
Provide Juridical Data	3.20	X			
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			
Cold Movement Detection	3.15.8		X [7]		
Continue Shunting on desk closure (Enabling transition to Passive Shunting mode)	5.12.4	X			
Manage “Stop Shunting on desk opening” information	4.4.20.1.8 4.4.20.1.9	X			
Manage Virtual Balise Covers	3.15.9	X			
Advance display of route related information	3.15.10	X			

Table 20 Relating Functions from SUBSET-026

[5] 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.
[6] RBC handover might also be relevant for VL, e.g. digital map downloads
[7] Depends on technology used. In general, VL could provide input for cold movement detection

Appendix E Overview of available specifications useful for OCORA

The table in this appendix contains an overview of available specifications, useful for the OCORA architecture and design work. The table attempts to assign the different specifications to the respective OSI layer(s), but this does not imply that a listed specification is applicable (to the assigned OSI layer) in the OCORA contexts. It just indicates that there is (useful) information in the listed specification that could be helpful for the OCORA architecture and design work. The table is a working instrument and not complete at this point in time. It is updated as information becomes available. The priority column indicates the priority an interface has within OCORA (1 = high priority / 3 = low priority).

Red indicates mandatory interface specifications

{ } indicates that the specification is not released yet

E1 Hardware interfaces - available specifications useful for OCORA

IF ID	IF Name	OSI Layer 1	OSI Layer 2	OSI Layer 3	OSI Layer 4	OSI Layer 5	OSI Layer 6	OSI Layer 7	Remark	Priority
101	UIDR - Driver	-	-	-	-	-	-	-		-
103	DMI - Driver/Technician	-	-	-	-	-	-	-		3
104	MT - Technician	-	-	-	-	-	-	-		3
110	TRU - Evaluator	-	-	-	-	-	-	-		3
120	VL-Sensors	-	-	-	-	-	-	-		-
130	LT-Antenna	-	-	-	-	-	-	-		-
131	BT-Antenna	-	-	-	-	-	-	-		-
132	NTC-Antenna	-	-	-	-	-	-	-		-
140	P-Sensors	-	-	-	-	-	-	-		-
150	EB / TCO / others	-	-	-	-	-	-	-		-
161	Cab Radio - Driver	-	-	-	-	-	-	-		-
162	GSM-R Voice Radio (Air)	-	-	-	-	-	-	-		-
181	GSM-R EDOR Radio (Air)	-	-	-	-	-	-	-		-
183	Public Radio (Air)	-	-	-	-	-	-	-		-
184	FRMCS Radio (Air)	-	-	-	-	-	-	-	TOBA responsibility	-
190	Vehicle Control System Network	SS 119, {SS 143}						-		1
195	Passenger Info System Network	-	-	-	-	-	-	-		3
197	UIC	-	-	-	-	-	-	-		-
300	UVCC Bus	**EN50170** SS 035		-	-	**SS 056** **SS 057**	**SS 037**	-	-	1

Table 21 Hardware interfaces (OSI layers 1-6)

E2 Functional interfaces - available specifications useful for OCORA

IF ID	IF Name	OSI Layer 1	OSI Layer 2	OSI Layer 3	OSI Layer 4	OSI Layer 5	OSI Layer 6	OSI Layer 7	Remark	Priority
201	UIDR - Driver	-	-	-	-	-	-	-		-
203	DMI - Driver/Technician	-	-	-	-	-	-	Refer to document [19]		3
204	MT - Technician	-	-	-	-	-	-	-		3
210	TRU - Evaluator	-	-	-	-	-	-	SS 027		3
220	VL-Sensors	-	-	-	-	-	-	-		-
230	LT-Antenna	-	-	-	-	-	-	**SS 044**		-
231	BT-Antenna	-	-	-	-	-	-	**SS 036**		-
232	NTC-Antenna	-	-	-	-	-	-	-		-
240	P-Sensors	-	-	-	-	-	-	-		-
250	EB / TCO / others	-	-	-	-	-	-	**SS 034** {SS 119}		-
261	Cab Radio - Driver	-	-	-	-	-	-	-		-
262	GSM-R Voice Radio (Air)	-	-	-	-	-	-	-		-
281	GSM-R EDOR Radio (Air)	-	-	-	-	-	-	**SS 037**		-
283	Public Radio (Air)	-	-	-	-	-	-	-		-
284	FRMCS Radio (Air)	-	-	-	-	-	-	-		-
290	Train Control System	-	-	-	-	-	-	**SS 034** {SS 119}		-
295	Passenger Info System	-	-	-	-	-	-	-		-
297	UIC	-	-	-	-	-	-	-		-
401	UIDR	-	-	-	-	-	-	-		3
403	DMI	-	-	-	-	-	-	{SS 121}		1
404	MT	-	-	-	-	-	-	-		3
410	TRU	-	-	-	-	-	-	**SS 027** {SS 140}		1
420	VLS	-	-	-	-	-	-	Refer to document [20]		1
430	LTM	-	-	-	-	-	-	**SS 026-7 & 8**		1
431	BTM	-	-	-	-	-	-	**SS 026-7 & 8** **SS 101**		1
432	STM	-	-	-	-	-	-	**SS 035 / 058** **SS 101**		1
440	PSs	-	-	-	-	-	-	-		3

IF ID	IF Name	OSI Layer 1	OSI Layer 2	OSI Layer 3	OSI Layer 4	OSI Layer 5	OSI Layer 6	OSI Layer 7	Remark	Priority
450	I/O Ports	-	-	-	-	-	-	**SS 034** {SS 119}		1
460	Cab Radio	-	-	-	-	-	-	-		3
480	MCG	-	-	-	-	-	-	-		2
490	Train Control System	-	-	-	-	-	-	**SS 034** {SS 119}, {SS 139}	OCORA Workstream #05	1
492	Train Integrity Monitoring System	-	-	-	-	-	-	**SS 034** {SS 119}		-
495	Passenger Info System	-	-	-	-	-	-	-		3
RCA-05	APS-MOT	-	-	-	-	-	-	-	Cooperation with RCA	3
RCA-06	APS-MT	-	-	-	-	-	-	**SS 026-7 & 8**	Cooperation with RCA	1
RCA-08	ATO-AT (IM)	-	-	-	-	-	-	{IRS 90940} {SS 126}	Cooperation with RCA	1
508	ATO-AT (RU)	-	-	-	-	-	-	-		
RCA-41	DM (IM)	-	-	-	-	-	-	-	Cooperation with RCA	2
541	DM (RU)	-	-	-	-	-	-	-		2
RCA-42	DCM (IM)	-	-	-	-	-	-	-	Cooperation with RCA	2
542	DCM (RU)	-	-	-	-	-	-	-		2
RCA-43	IAM (IM)	-	-	-	-	-	-	-	Cooperation with RCA	2
543	IAM (RU)	-	-	-	-	-	-	-		2
SFERA	SFERA	-	-	-	-	-	-	-	Cooperation with RCA	3

Table 22 Functional interfaces (OSI layer 7)

Appendix F Mapping OCORA with TOBA architecture

This Appendix provides initial ideas on the mapping between the OCORA and the TOBA architecture using the migration scenarios of the Cab Radio and ETCS.

F1 Cab Radio

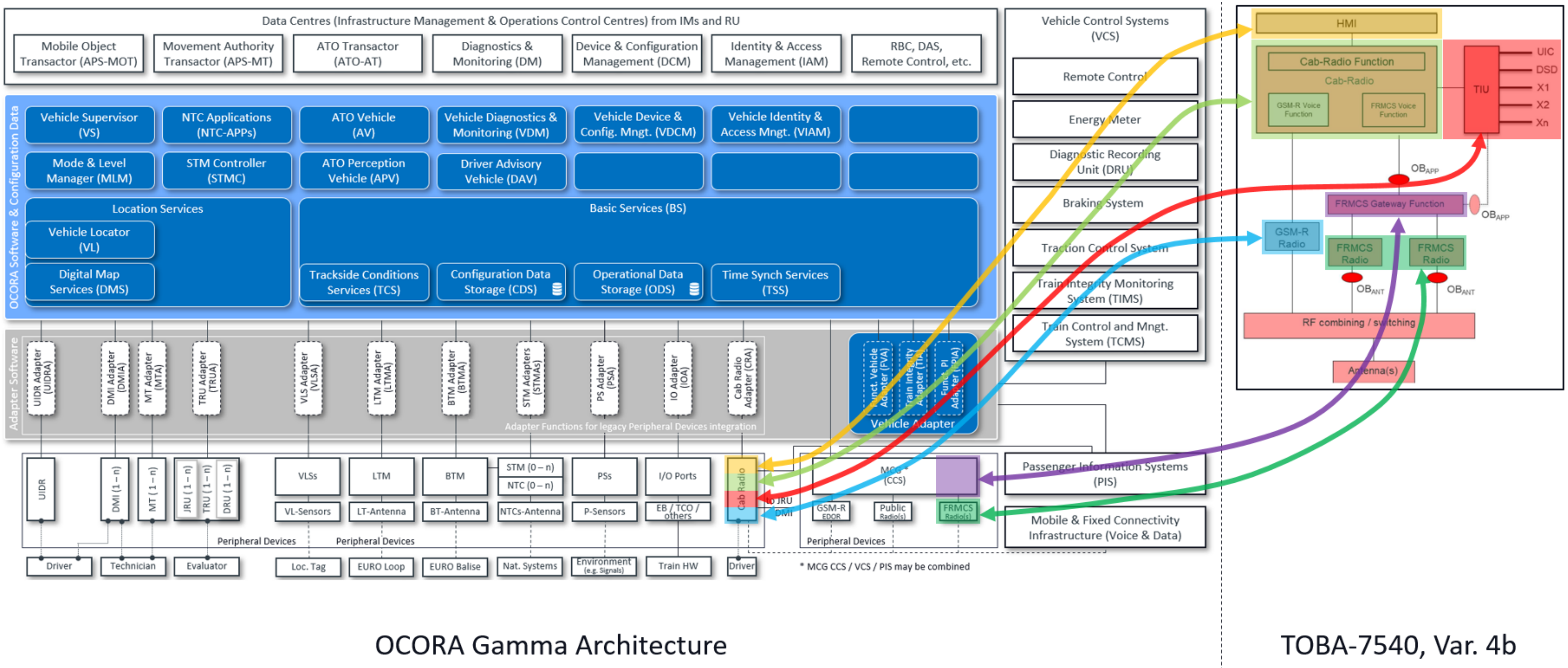

Figure 30 Mapping OCORA with TOBA architecture – Cab Radio

F2 ETCS

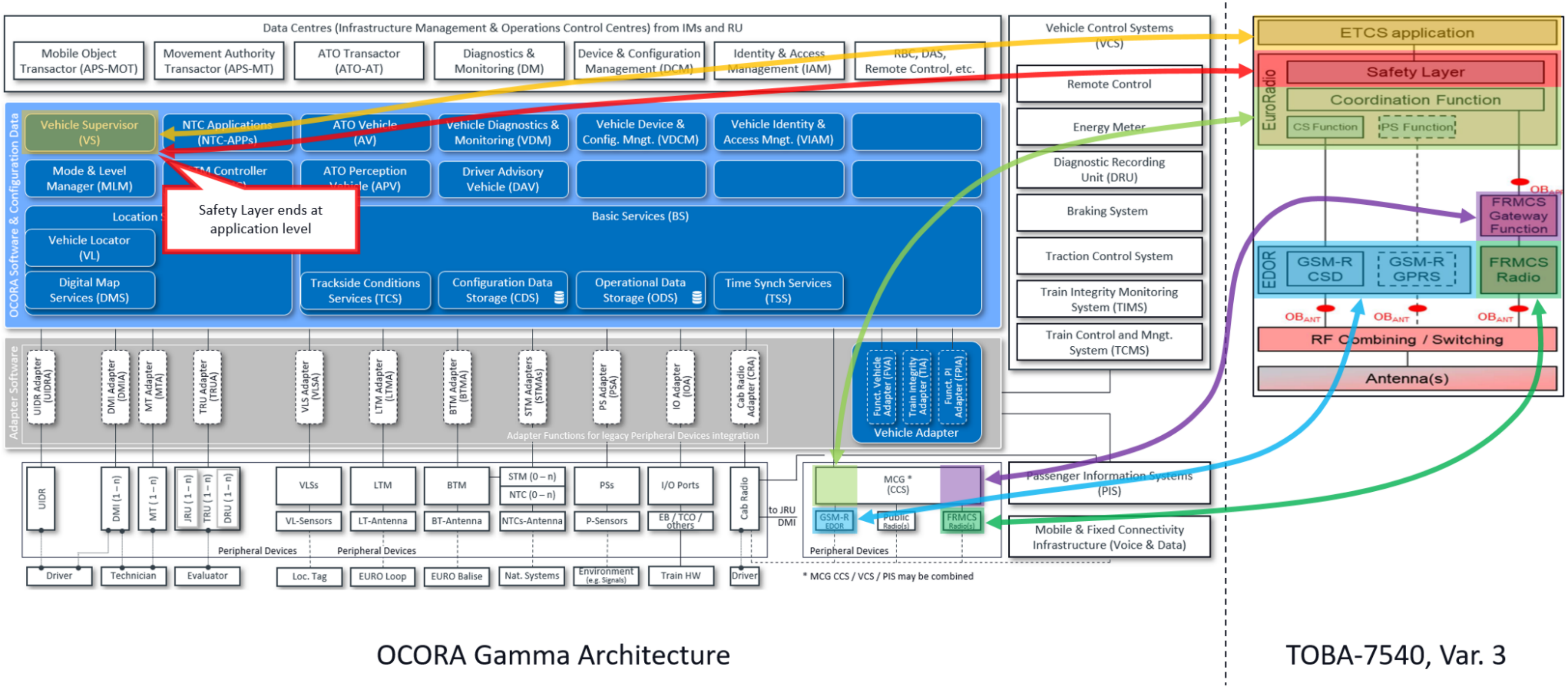

Figure 31 Mapping OCORA with TOBA architecture - ETCS

Appendix G Large scale graphics

G1 OCORA hardware components, scope, and external interface identification

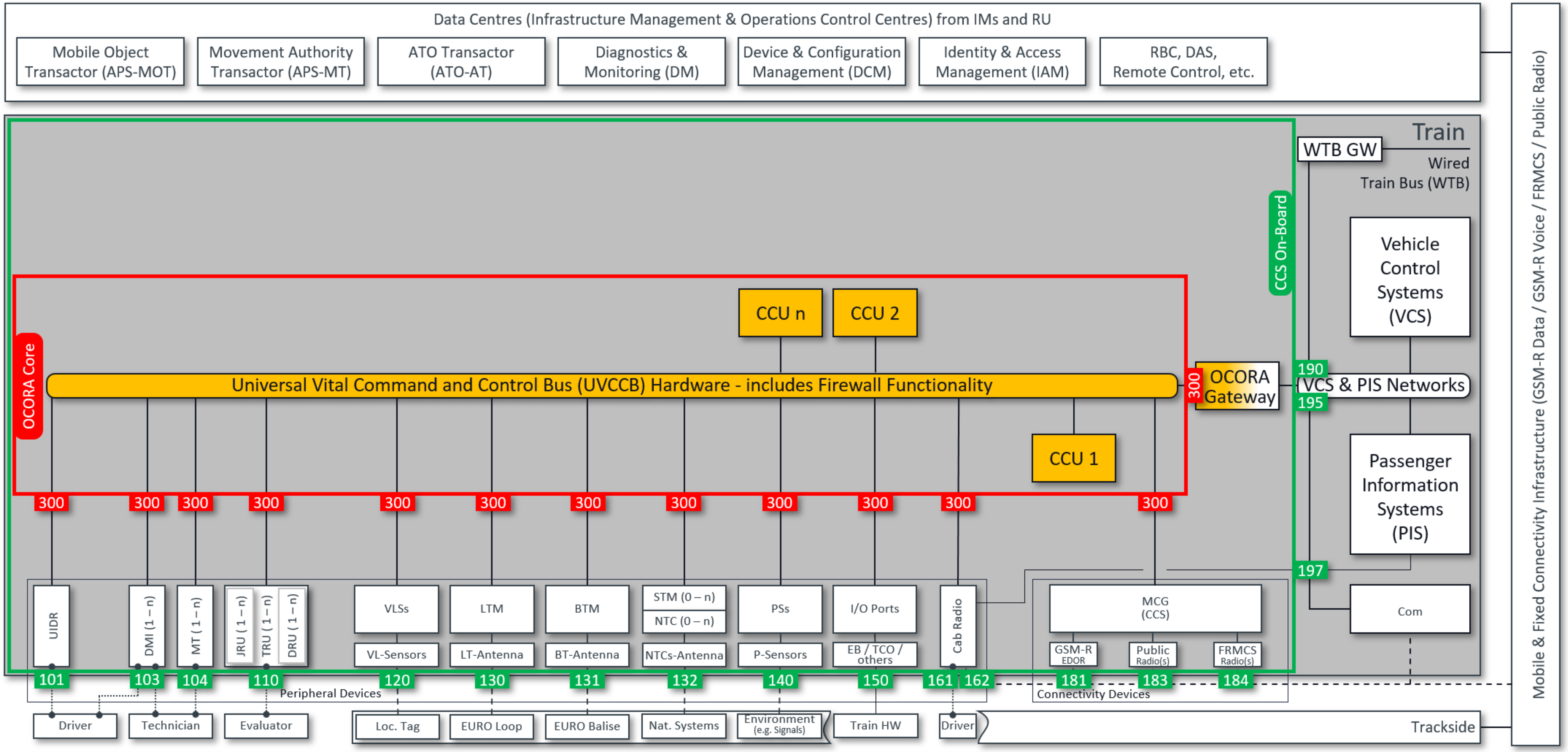

Figure 32 OCORA hardware components, scope, and interface identification

G2 OCORA functional components, scope, and external interface identification

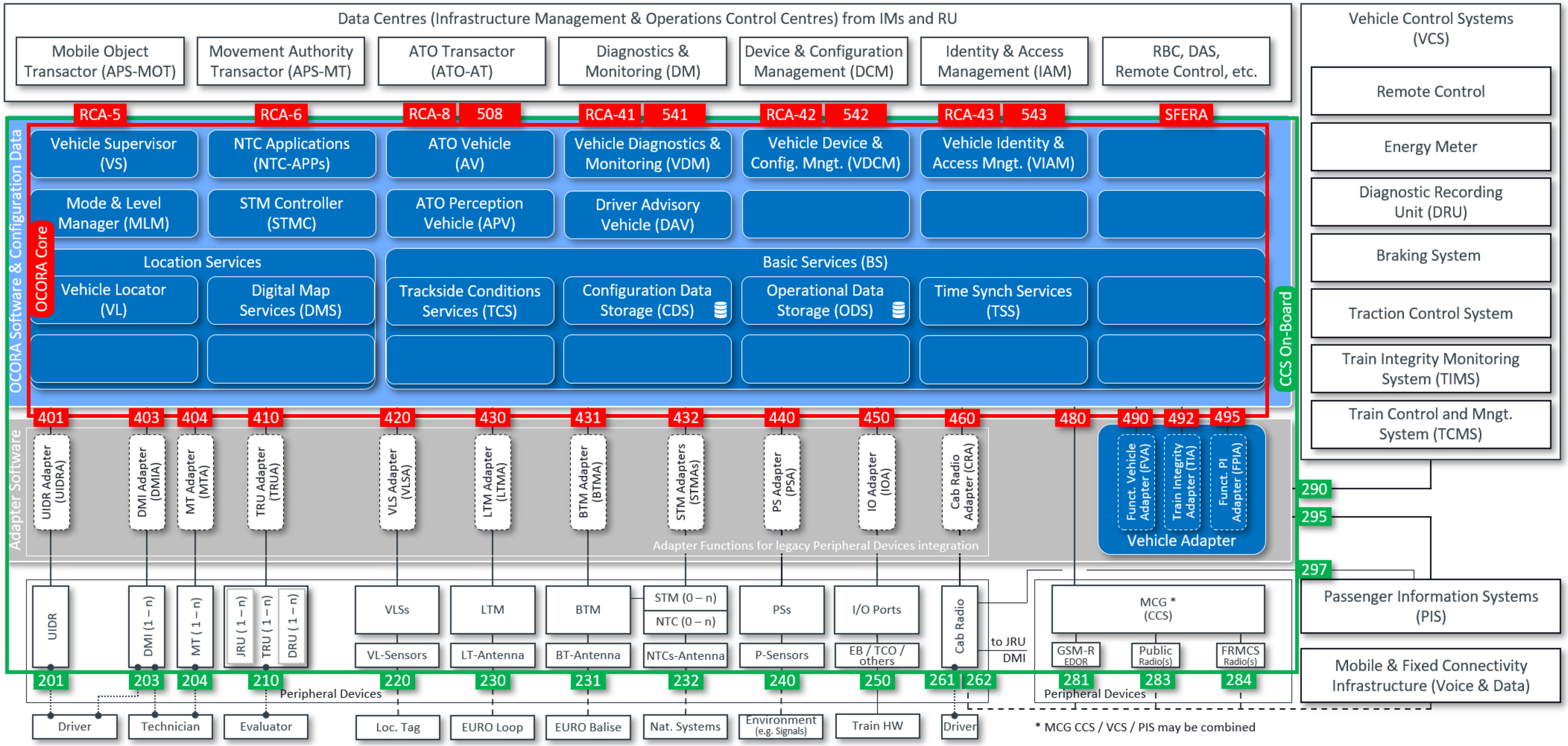

Figure 33 OCORA functional components, scope, and interface identification