OCORA

Open CCS On-board Reference Architecture

Concept

CENELEC Phase 1

Document ID: OCORA-TWS10-010

Version: 2.00

Release: R1

Date: 26.11.2021

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for Delta Release	RME	30-06-2021
2.00	Official version for Release R1	RME	26-11-2021

Table of contents

Table of figures

Table of tables

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references.

[1] OCORA-BWS01-010 – Release Notes
[2] OCORA-BWS01-020 – Glossary
[3] OCORA-BWS01-030 – Question and Answers
[4] OCORA-BWS01-040 – Feedback Form
[5] OCORA-BWS02-010 – Executive Summary Slide Deck
[6] OCORA-BWS02-021 – Program Slide Deck
[7] OCORA-BWS02-030 – Technical Slide Deck
[8] OCORA-BWS02-040 – Program Posters
[9] OCORA-BWS02-050 – Technical Posters
[10] OCORA-BWS03-010 – Introduction to OCORA
[11] OCORA-BWS03-020 – Guiding Principles
[12] OCORA-BWS04-010 – Problem Statements
[13] OCORA-BWS08-010 – High Level Methodology
[14] OCORA-BWS08-020 – High Level Tooling
[15] OCORA-TWS05-010 – Requirements – Management Guideline
[16] OCORA-TWS05-020 – Stakeholder Requirements
[17] OCORA-TWS05-021 – Program Requirements
[18] OCORA-TWS06-010 – (Cyber-) Security – Project Security Management Plan
[19] OCORA-TWS06-020 – (Cyber-) Security – Guideline
[20] OCORA-TWS07-010 – Modular Safety – Strategy
[21] RCA.Doc. 2, Beta.1, RCA Architecture Overview
[22] EN 50126-1:2017-10 – Railway Applications – The Specification and Demonstration of Reliability,

Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

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

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

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

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

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

[28] TS 50701 - Railway application - Cybersecurity

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

[30] Application Guide - GUI/CCS TSI/2019

[31] SUBSET-026: System Requirements Specification

[32] SUBSET-091: Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2

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

[34] ERA_ERTMS_015560

[35] ERTMS User Group Document 97E2675B

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

Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g., SUBSET-026 [31]). We always reference to the latest available official version of the SUBSET, unless indicated differently.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to cover the CENELEC Phase 1 activities defined in EN 50126-1 [22] (see Figure 5). It presents the frame of the OCORA initiative and project through the following elements:

- Scope, context, and purpose of OCORA (initiative, project, deliveries) in chapter 2
- Presentation of the scope, context, purpose environment of the System in chapter 3
- Identification of previous RAMS requirements and past RAMS performance of similar and/or related systems in chapter 4 and 5
- Presentation of the current RAMS policy and targets of the relevant railway duty holders in chapter 6
- Presentation of the safety legislation in chapter 7
- List of assumptions and justifications used to build this system concept in chapter 8
- List of open issues in chapter 9, which are needed to be solved in the next phase

1.2 Applicability of the document

This concept is developed as part of the OCORA activities within the OCORA initiative. This concept is valid for the OCORA project and describes the system under consideration (SuC).

The authors are responsible for creating, updating, and managing of this document.

The validity of this document is regulated at least for the entire duration of the project and at most by the defined retention requirements from the project.

The document represents the current state of the concept and if necessary, it will be further developed in consecutive releases.

1.3 Context of the document

This document is published as part of the OCORA release R1, together with the documents listed in the release notes [1]. It is the first release of this document.

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 the OCORA initiative we recommend to read the Introduction to OCORA [10], and the Problem Statements [12]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

1.4 Abbreviations and Terms

OCORA project uses a common Glossary [2]. All abbreviation and terms used in this document are defined in in this document.

2 Context, Scope and Purpose of OCORA

2.1 Context of OCORA

The deployment of ERTMS is today a reality in the EU with 15,000 km of lines to be equipped by 2023. ERTMS is however facing major challenges:

- Current control command and signalling on-board solutions in Europe are driving significant investment and maintenance costs
- Those solutions did not consider the differences in life cycles between its constituents or parts
- The ERTMS specifications written in natural language are error-prone with different possible interpretations from different suppliers
- Major innovations around the ETCS core are to be deployed in the next decade to boost the railway sector efficiency (i.e., ATO, fail-safe train localization, next radio communication system, …)

Recognizing that a coherent, modular, upgradeable, interchangeable, reliable, and secure system architecture is paramount to overcome these challenges for the overall control command and signalling system of the European railway sector, the signatory parties intend to establish the Open CCS On-board Reference Architecture (referred to as “OCORA”), in coherence and complementarity with the trackside Control, Command and Signalling subsystem.

To keep up competition with modal competitors, investing heavily in digitalisation and automation, railways rapidly must embed innovative technologies in their physical assets, planning systems and operations. Digitalisation and automation are the prerequisites for boosting productivity, controlling cost and risk levels, and improving performance.

That is why OCORA deems the fast integration of the game changers in the CCS domain of imperative importance and intends to gradually extend the grade of automation of heavy rail to the domain of fully automatic, unmanned operation (since decades business as usual in light rail).

The European railway community has identified ATO over ETCS to be the preferred solution for implementing ATO in heavy rail environments. At the same time, it recognizes the drawbacks of the current ERTMS implementation process which encompass high development and investment costs for suppliers and customers, performance issues and considerable technical, operational, and financial risks.

This raises the question as to what needs to be accomplished to provide railway transportation a sound and future proof economic foundation and how this can be achieved.

So, the OCORA project has been started by OCORA members (i.e., OCORA initiative) with the goal to define how the CCS on-board can be developed in the next decade to satisfy the needs and requirements of railway companies engaged in the transportation of passengers and goods.

Depending on the context, OCORA may have different meaning. To avoid misunderstandings, some definitions are proposed to avoid misunderstandings.

- **OCORA initiative/collaboration** refers to the RU group responsible for the OCORA project development.
- **OCORA program** refers to the overall work (projects and workstreams) done by the OCORA initiative.
- **OCORA project** refers to the teamwork and organisation aiming to develop the OCORA deliverables.
- **OCORA deliverables** represent the documentation that will come out of the OCORA project and will be spread to realize call for tenders by the RU for their future CCS on-board solutions according to OCORA

2.1.1 OCORA Initiative

The below shown members collaborate on the development of an open reference architecture for on-board command-control and signalling system that complies with the mutually agreed OCORA objectives.

Figure 1 OCORA Initiative

Collaboration takes place in workstreams. Each workstream is responsible for specific tasks, topics, or issues. Workstreams and participating experts are appointed by the OCORA management team.

The OCORA initiative/collaboration is organised among the following bodies:

- The SteeCo is defining the OCORA strategy and organise funding.
- The Core Team is responsible for the operational management.
- The Workstream Teams are responsible for the development of topic specific content

This document focuses on the OCORA project “OBU Development Project” and beside being the concept document from phase 1, it also presents the strategy defined by the OCORA initiative to produce the OCORA deliverables.

2.1.2 OCORA Program

The work and the projects within the OCORA Initiative are coordinated, steered, and managed in the OCORA Program.

Dedicated OCORA Workstreams are in place to solve specific issues and develop certain aspects of the OCORA Program. Figure 2 shows the overview of all Workstreams from the OCORA Program.

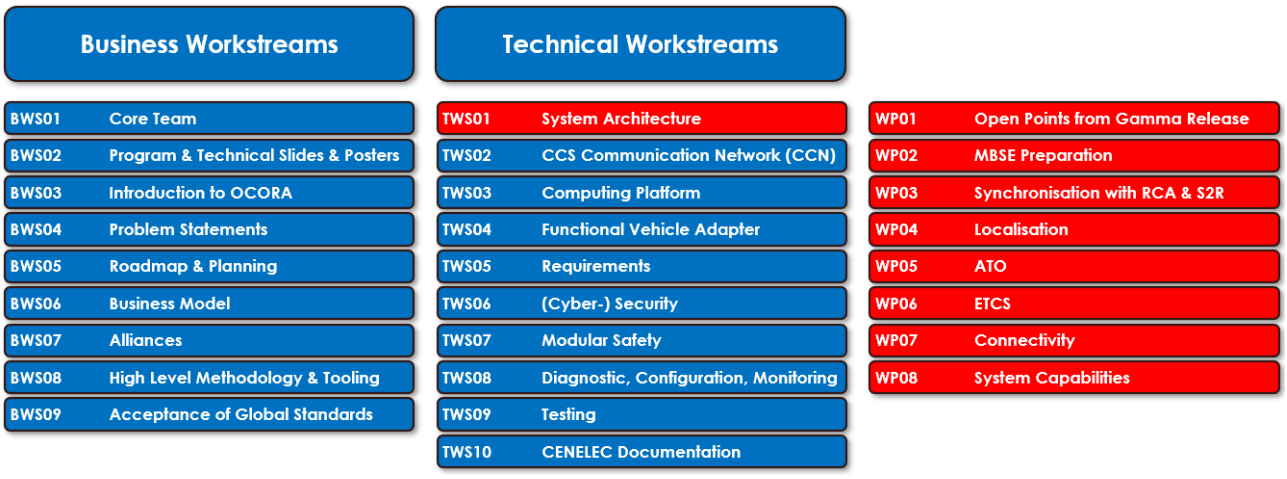

Figure 2 OCORA Program Workstreams and Work Packages

As shown in the Figure 2 the OCORA program has business and technical workstreams to cover all necessary aspects from the OCORA program. The system architecture workstream is divided in nine work packages to enable parallel progress on different topics related to the architecture development.

2.1.3 OCORA Project

The OCORA initiative aims to define an open CCS on-board reference architecture. The OCORA shall deliver a comprehensive and coherent set of specification (architecture and interfaces) for a modular CCS on-board environment that will be published in consecutive OCORA releases. These specifications shall serve as a voluntary format for tender templates, supporting companies currently engaged in procurement activities or soon starting procurement programmes.

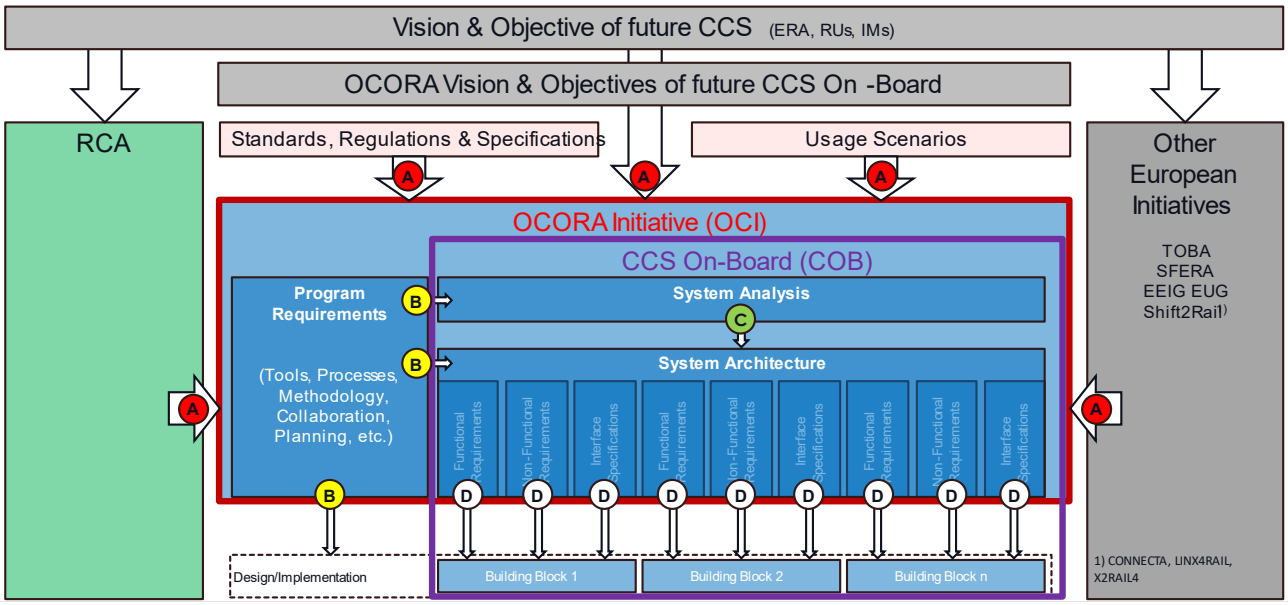

Figure 3 OCORA Requirements Structure from Project Input Sources

Figure 3 shows the different incoming information for the OCORA development project. They are described in more detail in the following subchapters.

The OCORA document Requirements Management Guideline [15] provides the definition shown in Figure 3. It gives an overview on how OCORA plans to structure and handle its requirements until the requirements on subsystem level are developed (D-level).

In the document Requirements Management Guideline [15] the levels of the requirements are described as following:

According to Figure 3, the **Stakeholder Requirements (A)** are the foundation of OCORA requirements. They contain all requirements towards the OCORA Program and the envisages CCS On-board System. In essence they include:

- OCORA Vision and Objective of future CCS On-board as described in the OCORA Introduction [10]
- Regulations / Norms and Standards
- Operational Scenarios
- Requirements from external Stakeholders (e.g. RCA, ER JU / Shift2Rail, EULYNX, EUG, TOBA, SFERA, etc.)

Program Requirements (B) are focusing on how the OCORA program defines tools, processes, methodology, collaboration, planning, etc. They are to be used within the program and to be considered during the system analysis and the system architecture work.

System Requirements (C) are defining the CCS On-board system; hence they describe how the system is developed in the MBSE System Analysis (RCA & OCORA), considering the A- and B-Level Requirements.

The Building Block Requirements (D) are in regard to the OCORA building blocks, developed in the MBSE System Architecture (logical / physical), considering the MBSE System Analysis. The resulting documentation form the OCORA inputs for tender templates, together with the applicable program requirements.

The document Stakeholder Requirements [16] provides the collection of all Stakeholder Requirements in a structured manner and it follows the document Requirements Management Guideline [15], which defines the OCORAs requirements management and the requirement engineering process. The complete set of OCORA deliverables will be according to CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22].

2.1.3.1 Vision & Objectives of future CCS from ERA

ERA does not provide a vision and objective of future CCS directly, but mandates UNISIG (Union Industry of Signalling) to develop and provide visions of future CCS architecture solutions. Chapter 11 of the document "Concept for the evolution of the on-board CCS architecture from 21.03.2021" shows the architectural drawings based on the analysis and guiding principles from the document and separates it in short-term, mid-term, and long-term solutions. Especially the long-term solution gives a vision of the future CCS solutions.

The long-term proposal will be the definition on the on-board CCS subsystem for a future CCS TSI, probably in force in 2025 or later. It will be the target system (note: two of the European railway sector's goals concerning the on-board CCS subsystem are protection of investment and an adaptable approach to deal with system upgrades) as it fully standardizes all interface between CCS and TCMS among the interchangeable elements (excluding legacy NTCs) based on the CCS one common bus.

For the time being the long-term proposal can only be regarded as a vision, as some fundamental architectural decisions must be made. But the vision already demonstrates a reasonable level of modularity and what will be possible with respect to the target system:

The ETCS on-board as the focal point of the on-board CCS subsystem comprises all SIL4 components, which includes the EVC, odometry sensors and the Eurobalise antenna.

For new vehicles, the EVC could be limited to

- a safe Dig-I/O for safety-related purposes.
- proprietary and harmonized interface (ProfiBus) for the interface to NTCs.
- API based on ECN for future enhancements.

The ETCS indication on a DMI is an independently certifiable function provided by a train display system (as defined by Subset-121) and is not part of the ETCS-onboard interoperability constituent.

Based on the ETCS on-board's API the non-safety related functionality of the Euroradio protocol could be provided by an individual and interchangeable element called "Euroradio gateway". The "Euroradio gateway" serves to separate the non-safe communication through FRMCS from the safe automatic train protection through ETCS.

More information about vision and objectives from ERA can be found in the document Stakeholder Requirements [16].

2.1.3.2 European Initiatives

RCA represents the main European workstream interfacing with OCORA. However, additional ones may have a direct link (e.g., shared interface) with the OCORA project. The following list, which represents the major European Initiatives (not complete) has been initiated:

- TOBA in terms of relevant interfaces and requirements exchange
- SFERA (Smart communications For Efficient Rail Activities) in terms of relevant interfaces
- EEIG ERTMS USERS GROUP in terms of localization
- Shift2Rail:
    - CONNECTA
    - LINX4RAIL
    - X2RAIL

A more detailed description can be found in the document Stakeholder Requirements [16]. The relevance, kind of input from and necessary interactions with the other European initiatives will be analysed in CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22].

2.1.3.3 Operational scenarios

The operational scenarios can be found in the document Stakeholder Requirements [16]. These scenarios will be analysed in CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22].

2.1.3.4 Vision & Objectives of future CCS from OCORA

OCORA members agreed to collaborate in achieving the following specific objectives:

- To define an Open CCS on-board reference architecture by e.g.:
  - Open standardisation of the ETCS/ATP and ATO train interfaces and functions and other on-board subsystems as plug and play solutions (e.g., a reference runtime platform with open interfaces).
  - Establishing the principles and necessary requirements of the OCORA initiative.
  - Aligning initiatives and ideas already started and find synergies to align scarce resources.
  - Streamlining industrialisation processes in particular the certification.
- To foster and develop the open ETCS/ATP source initiative by utilizing and benefitting from the existing results of the “openETCS” initiative and sharing common understanding on this initiative.
- Validate the viability and relevance of the OCORA approach by using e.g., demonstrators.
- To promote the use of OCORA for the CCS on-board solutions in Europe to make it more cost effective, reliable, safe, and secure by e.g.:
  - Ensuring consistency on a railway system scale between OCORA and other similar initiatives. This will be done in close coordination with sectoral organizations (e.g., CER, EIM, EPTTOLA, etc.), and close cooperation with joint undertakings, already in charge of defining certain aspects of the ERTMS (e.g., Shift2Rail, EuG, EULYNX, UNISIG, JPCR, UIC, RCA, etc.)
  - Building consensus and getting support from railway companies by means of regular information towards sectoral associations (e.g., members of the group of representative bodies)
  - Facilitating the industrialisation of OCORA results, notably certification, through input to and discussions with associations, sectorial organizations, manufacturing companies and joint undertakings (e.g., UNIFE, UNISIG, Shift2Rail, ERL - European Reference Laboratories, etc.)

It must be noted that the OCORA project does not redefine the existing functional behavior of ERTMS components that are documented into the SUBSETs called by the TSI CCS [29]. OCORA deliverables constitute a complementary set of documents that specifies the interfaces and new functionalities (listed in CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22]) to reach the goals and objectives.

2.1.3.5 Standards

The detailed list and structure of standards considered for the OCORA project is presented in chapter 7 (Safety Legislation).

2.1.4 OCORA Deliverables

As shown in the figure below the core deliverables from the OCORA project are the specifications for requirements and testing. Additionally, guidelines and instruction documentation are already available or will be created from the OCORA project. The portfolio of guidelines and instructions will be increased and updated with each OCORA release. The aim is to cover the most relevant domains.

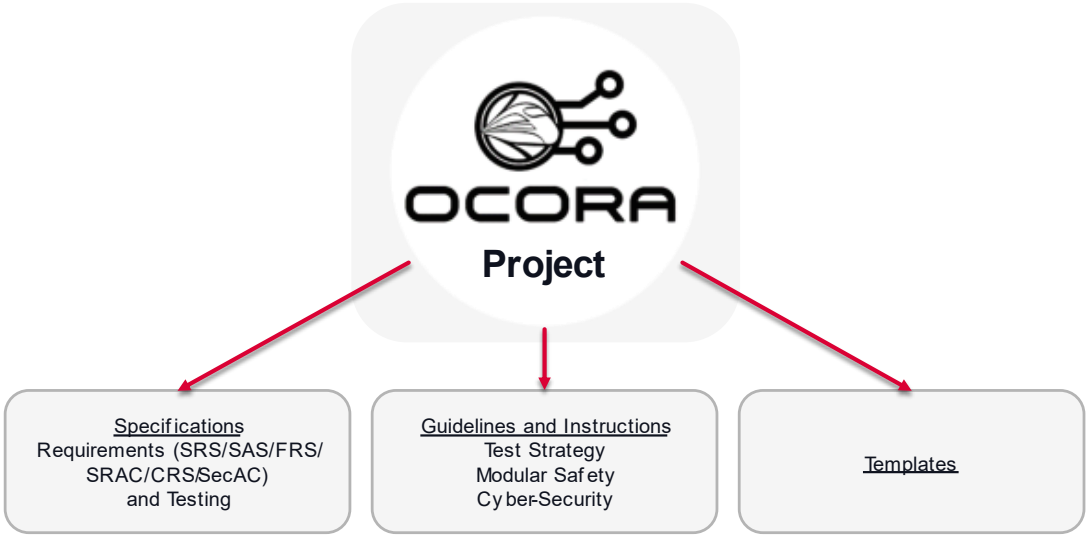

Figure 4 OCORA Project Deliverables

As presented above the OCORA project defines OCORA deliverables that will be used to realise the future CCS on-board solutions according to TSI CCS [29].

OCORA deliverables are composed of:

- Functional and non-functional (e.g., RAMSS) requirements corresponding to the future referenced architecture
- Instructions and guidelines that will support the different stakeholders involved in the development of OCORA compliant CCS on-board systems
- Templates related to CENELEC development phases 1 to 5 according to EN 50126-1 [22] that can be used by any organisation aiming at realising OCORA compliant CCS on-board systems

2.1.5 OCORA Process

To reach the apportioned requirements on subsystem level the OCORA project has tailored the CENELEC process to its needs, which is shown in Figure 5 and will be followed until the defined deliverables are completely developed. Since the output of OCORA comprises a set of specifications, the current scope of OCORA is limited to phases 1-5 (see Figure 5) of EN 50126-1 [22]. The OCORA document High Level Methodology [13] provides the definition shown in Figure 5.

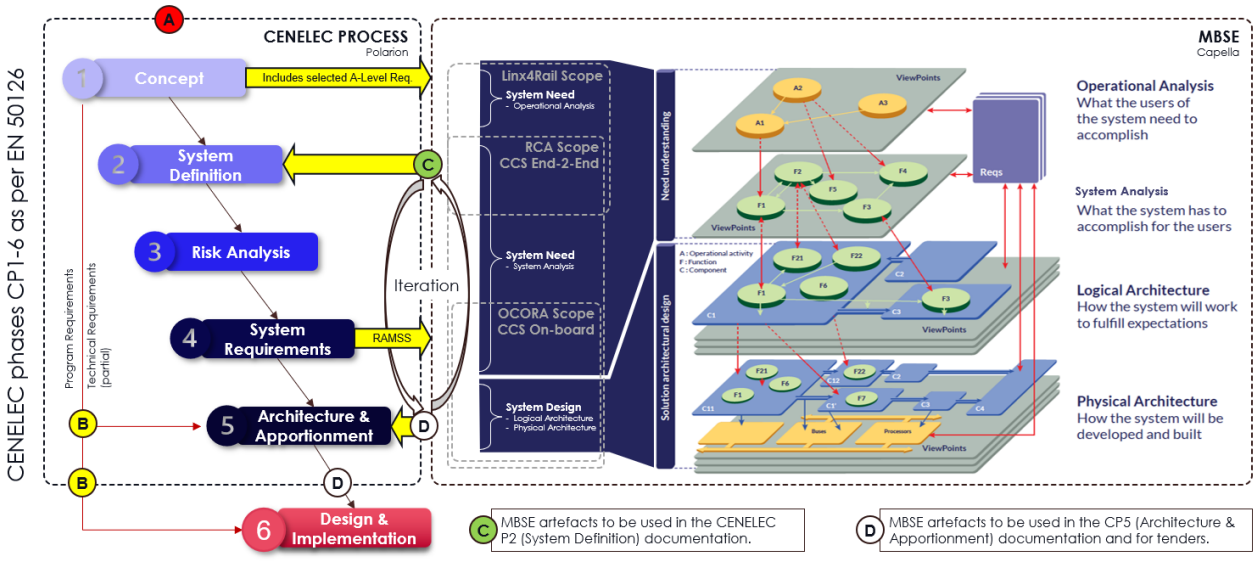

Figure 5 Tailored CENELEC Process

The following main interaction steps have been identified:

1. Based on A level “Stakeholder Requirements” the CENELEC Phase 1 “Concept” is developed
2. Based on CENELEC Phase 1 “Concept” and the Linx4Rail “System Need” definition the “Operational Analysis” and the “System Analysis” will be carried out from an end-to-end perspective lead by RCA supported from OCORAs CCS on-board subject matter experts
3. C level “System Requirements” are generated artefacts out of the two MBSE layers “Operational Analysis” and the “System Analysis” and are used as basis for the CENELEC Phase 2 “System Definition”
4. The subsequent CENELEC Phase 3 “Risk Analysis” and Phase 4 “System Requirements” are developed
5. Based on the two MBSE layers “Operational Analysis” and the “System Analysis” and the CENELEC Phase 4 “System Requirements” including all RAMSS aspects the “Logical Architecture” and the “Physical Architecture” are developed
6. D level “Building Block Requirements” are generated as artefacts out of the two lower MBSE layers “Logical Architecture” and “Physical Architecture”
7. Respecting the B level “Program Requirements”, the MBSE System Design output, the CENELEC Phase 5 “Architecture and Apportionment” collects the results
8. D level “Building Block Requirements” serve as input to tender templates for specific projects

Please note, the related tools (Polarion, Capella) to perform these interaction steps can be found in the document High Level Tooling, [14].

The requirements and testing specification on subsystem level will be an output from phase 5 of the OCORA tailored CENELEC process shown in Figure 5.

Following that, any RU will be able to implement a OCORA compliant systems, based on the OCORA deliverables. The following figure shows the relation between the OCORA project (yellow area) and the future stakeholders involved in the implementation of such an OCORA compliant system.

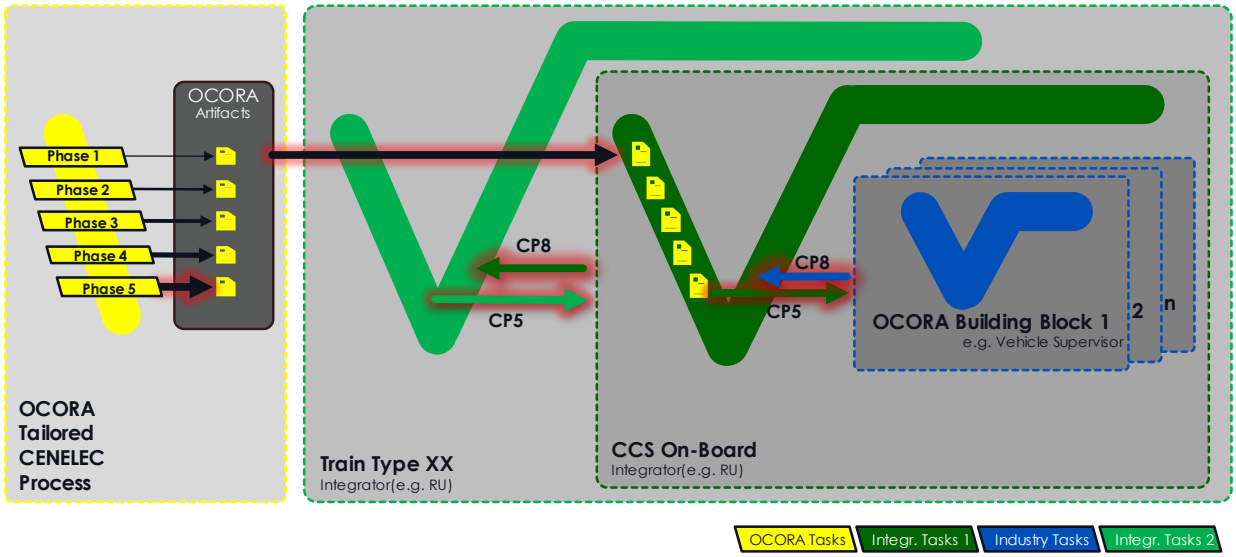

Figure 6 OCORA in context of the relevant projects

Figure 6 demonstrates the OCORA project (yellow area) with its deliverables (OCORA Artifacts) supporting a CCS On-board system integration project (dark green) with its artifacts.

The CCS On-board system consist of different subsystems and components (blue), which are integrated as part of the CCS On-board project (dark green). The CCS On-board is a subsystem of a train and needs to be integrated (dark green CP8 arrow) in another application (train level, light green).

2.2 Scope of OCORA

The OCORA project covers the 'on-board control-command and signalling' subsystem of a vehicle as defined in TSI CCS [29].

In addition to the current scope defined by TSI CCS [29], new functionalities are also in the scope like FRMCS and ATO.

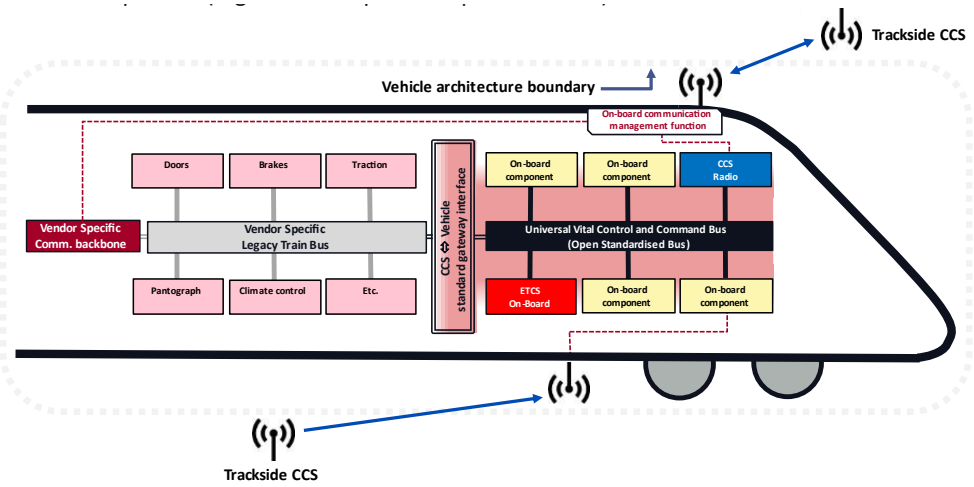

Figure 7 OCORA project scope

From system view the scope of the OCORA project is presented by the pink filled square including the gateway function to the vehicle legacy train bus, the universal vital control and command bus (UVCCB), the CCS radio function, the ETCS On-board function and related On-board component functions on the picture above.

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.

To identify the scope, OCORA has developed a hardware block diagram Figure 14. The diagram identifies the CCS On-Board and the OCORA Core scope.

The OCORA project is developed according to CENELEC EN 50126-1 from phase 1 to 5 (see Figure 5). The end of the OCORA project corresponds to the OCORA deliverables according to CENELEC phase 5 outputs.

2.3 Purpose of OCORA

The focus of OCORA is to standardise technical interfaces of signalling systems and behaviour of the onboard unit (see chapter 2.4 for the details) to open markets, accelerate innovations, and achieve economies of scale. OCORA aims to deliver assured generic functional interface specifications for a range of signalling interfaces. OCORA is intended to produce outputs (primarily interface specifications) that will be acceptable by all partner organisations (and their corresponding National Safety Authorities).

OCORA acts according to the principles defined in the memorandum of understanding. In the following the key principles from OCORA, which have to be applied during the development process are described in more detail

- OCORA is first and foremost a technical collaboration platform for its members. OCORA output will be made available to any stakeholder of the railway community.
- OCORA acts in full conformity with existing competition law under any circumstances and within the existing sectoral regulatory framework. CR proposals formulated by OCORA, will e.g., be registered for further treatment through existing channels like CER or EUG.
- Although OCORA aims at standardisation of the on-board CCS function, it does not envisage to set up a formal, “de iure” standard. However, OCORA will develop for its members and third parties, specifications for procurement purposes, following the examples of e.g., EULYNX.

In the process of developing the OCORA project, the principles defined in the memorandum of understanding have been developed further to clearly communicate what OCORA aims to achieve (see Figure 8).

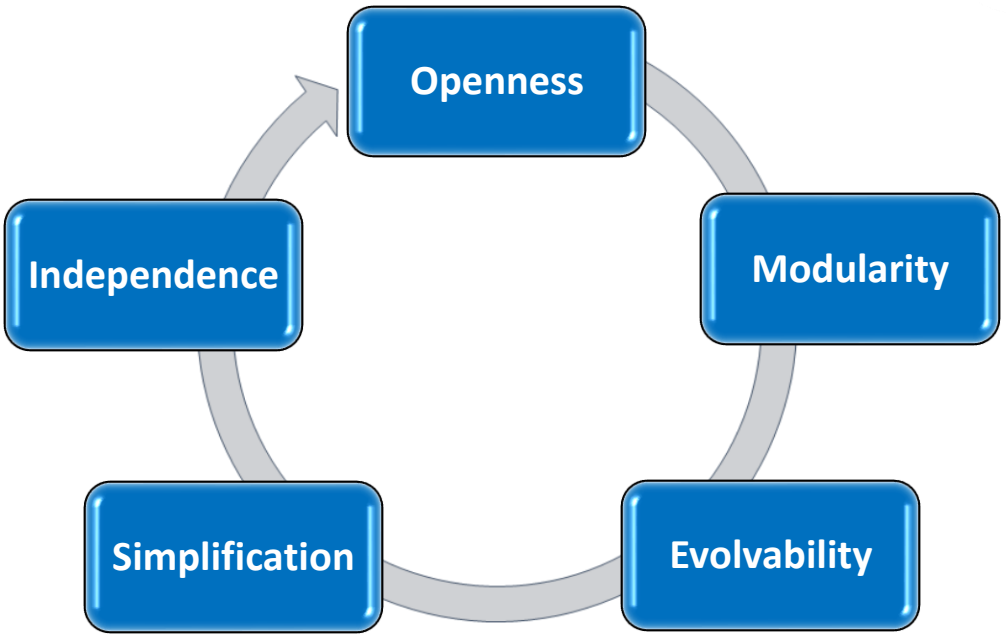

Figure 8 OCORA key principles

- **Openness**: OCORA is an open collaborative technical platform open to all railway companies. This includes IM's and RU's. It is based on sharing and making publicly available its deliverables for the benefit of the railway sector.
- **Modularity**: OCORA intends to decompose the on-board CCS subsystem into an optimal/reasonable number of standardized building blocks. System modularity is the basis for a modular safety approach and exchangeability, supporting different life cycles.
- **Evolvability**: Recognizing that continuous updates and upgrades are paramount to the railway digitalization, OCORA intends to introduce secure upgradability and interchangeability to speed-up the integration of future innovations in a flexible manner and to provide a solid basis for introducing game changers such as FRMCS or ATO.
- **Simplification**: OCORA plans to isolate in its architecture the functional blocks that will become obsolete in the foreseeable futures (e.g., GSM-R, class B systems, current Balise technology). This is the basis to easily simplify OCORA based implementations once the respective functions are not needed anymore.
- **Independence**: OCORA intends to minimize the dependencies between different building blocks and components, such as dependencies between hardware, software, and peripherals. This provides the basis for a modular product-based CCS system approach.

Therefore, the purpose of the OCORA project 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.

2.4 OCORA Development Stages

According to the Introduction to OCORA [10] and the Technical-Slide-Deck [7], development steps are identified that OCORA is using to consecutively address actual topics.

2.4.1 Current Situation

This is the current situation, and the integrated proprietary CCS system is fully integrated in the proprietary vehicle environment, driving costs and risks and complicating obsolescence issue. No modularity is given (see Figure 9).

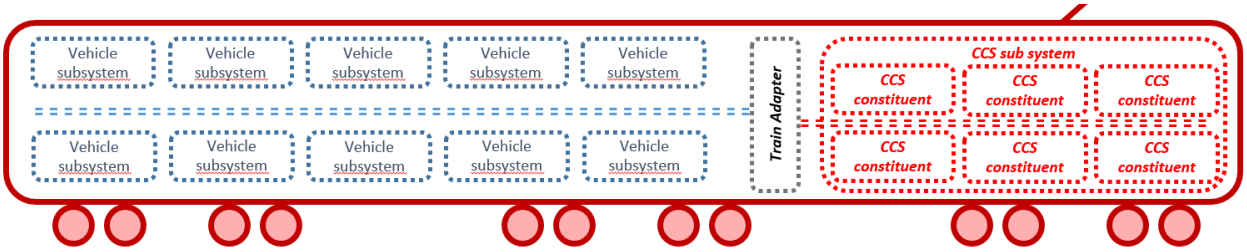

Figure 9 Current Situation

2.4.2 Preparing Retrofit Projects

In this step, the interface between the proprietary CCS system and the fully integrated proprietary vehicle environment is isolated, enabling exchange of the CCS environment without affecting the vehicle and vice versa, hence simplifying obsolescence issues. The aim is to have a generic and open interface between vehicle and ETCS system for future and existing fleet (see Figure 10).

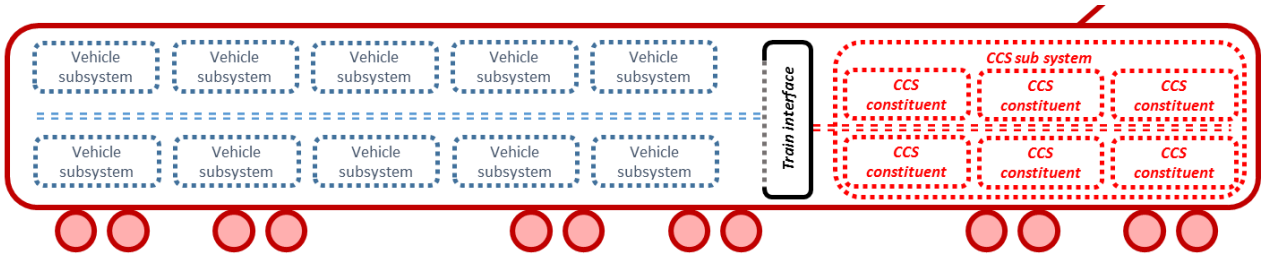

Figure 10 Decoupling of the CCS on-board and the vehicle

2.4.3 Modularisation of the CCS on-board

In this step, the CCS on-board will be decomposed into individual building blocks, connected by open interfaces and an open bus system (CCS communication network) allowing exchangeability between the building blocks without affecting either the vehicle or other CCS constituents (see Figure 11).

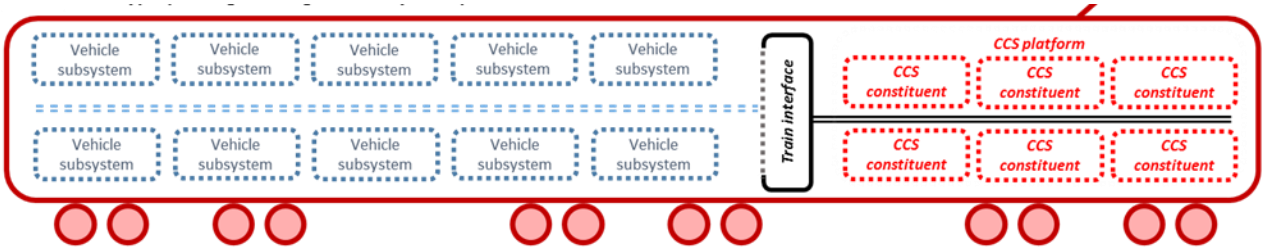

Figure 11 Modularization of the CCS on-board proper - UVCCB introduction

2.4.4 OCORA CCS platform

In this step, the core CCS functions will be organised on a generic platform that enables adding, removing, or changing functional applications without affecting the computing platform or runtime environment on which they are installed or the state of approval of non-affected parts of the system. This will facilitate fast and easy

software updates and upgrades of only those applications for which that is necessary, e.g. when requirements demand frequent updates of security software. Authorisation issues can be further simplified and contained.

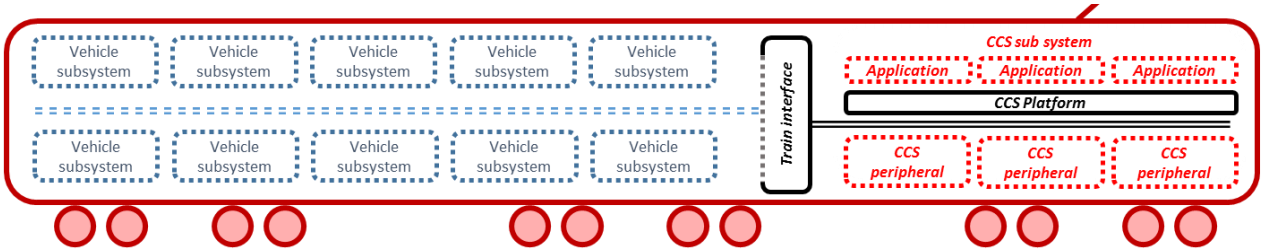

Figure 12 CCS platform with full plug and play capabilities for applications, hardware and peripherals

On the long term view, but already under scrutiny of OCORA and Shift2Rail Connecta, is the convergence of vehicle networks, consisting of one or multiple bus systems that integrate the CCS and vehicle bus systems.

Developments like GoA3 and GoA4 will require remote access and automated control of an increasing number of CCS and vehicle functions. Train interfaces allowing to connect to legacy bus systems may disappear but standardised secured communication interfaces to either physical or virtual building blocks, must be anticipated in order to facilitate decoupling. This affects safety approval, non-regression, cyber security and maintenance management, while allowing for innovation and fair competition. Obviously, existing technical standards should be improved or developed, the certification approval process should be revised, and new business models should be developed for both fleet owners, users and the supply industry.

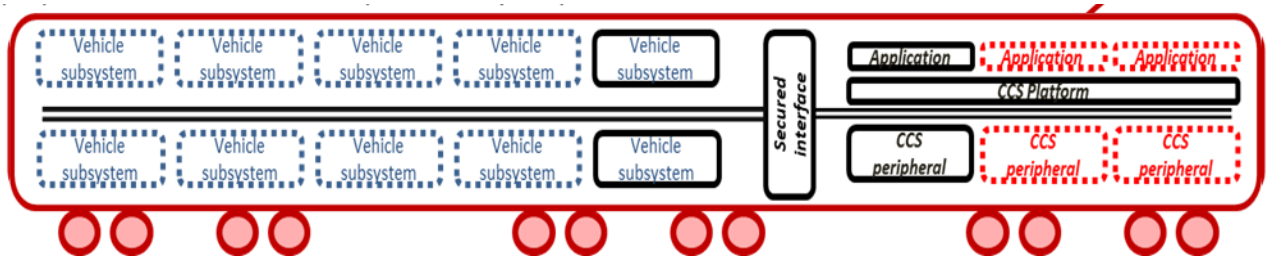

Figure 13 Future view: CCS building block integration supported by vehicle standardisation

3 Context, Scope and Purpose of the SuC

3.1 Context of the SuC

3.1.1 Approval Context

From approval point of view the SuC is a subsystem of a train, therefore it is a generic application, which needs to be integrated in another system (train/vehicle). As shown in Figure 6 the corresponding realisation project is the CCS On-board system (dark green project) from OCORA point of view.

3.1.2 Process Context

The question “is the SuC is already created as a subsystem during the development of another system” needs to be answered. During the development process of a generic application project on train level (mid green project in Figure 6) the SuC can be seen as a subsystem. Therefore, this must be considered during the development and requirements from the higher-level system must be realised during the development of the SuC.

From RCA point of view (CCS view) a vehicle, including the CCS on-board functions can be seen as a subsystem. As a result, from this understanding an own synchronisation work stream is in place to align system and functional view on CCS level.

3.1.3 Location Context

The system covers the whole equipment for CCS on-board and includes only equipment installed on the vehicle. It does not include any equipment being installed off-board.

3.1.4 Operational Context

The CCS On-board system is used as an essential and safety related subsystem of a train during ETCS or ATO operation. So, from operational point of view the SuC must deliver all ECTS and ATO functionalities. All operational scenarios related to the different operational modes derived from ETCS and ATO functionalities need to be analysed and realised by the SuC.

3.2 Scope of the SuC

The main scope of the CCS on-board system is to ensure safe vehicle movement on rails.

From component (hardware) perspective the system consists of the following elements:

- CCS computing unit (CCU): one or more computation units.
- Dedicated sensors and actors: according to the different functional needs/requirements.

Communication bus connecting the different components of the CCS on-board system (computation unit(s), the different sensors, and actors) between each other and to the remaining equipment on the vehicle (train control and management system, passenger information system). Within OCORA this bus is named CCS Communication Network (CCN).

Figure 14 presents an early version of a more detailed view of the SuC, which already includes and identifies some main components and subsystems:

- CCS On-board (green square) including a CCS Communication Network
- Train Adapter (blue square) including gateways

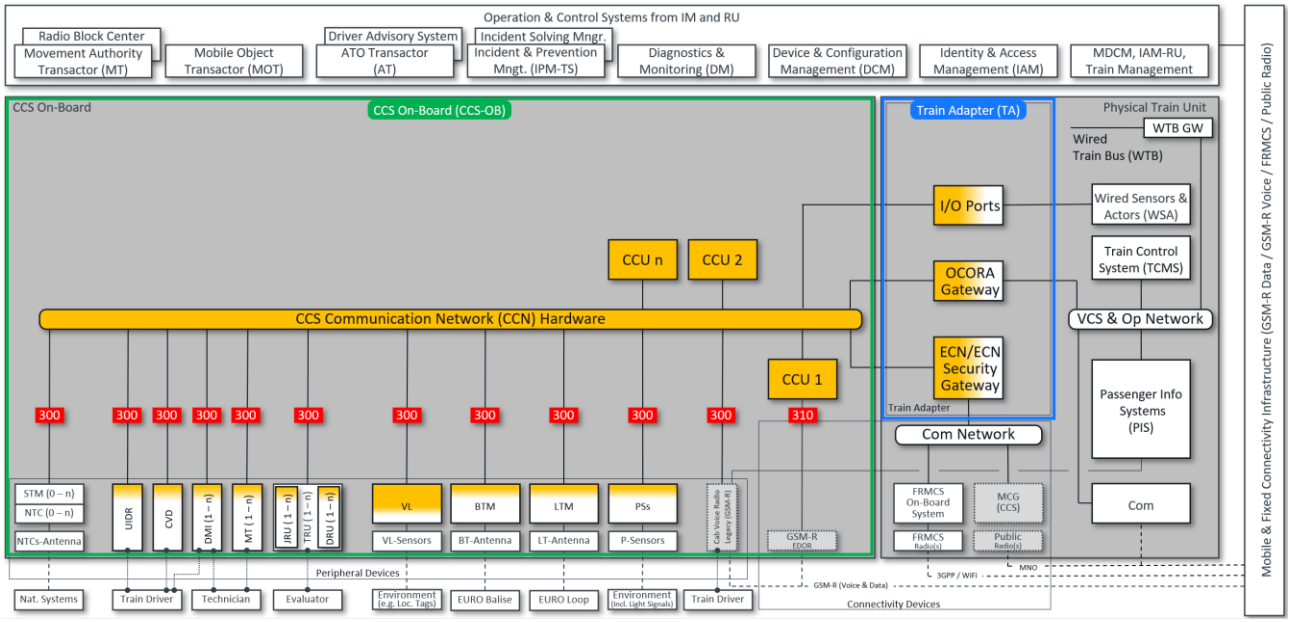

Figure 14 CCS On-board

From safety documentation perspective the system is:

- located on a train
- a subsystem of a train
- can consist of different subsystems
- needs to be integrated.

The following figure, despite being a proposal, shows an example of the hierarchy of the CCS on-board system with its subsystems and components:

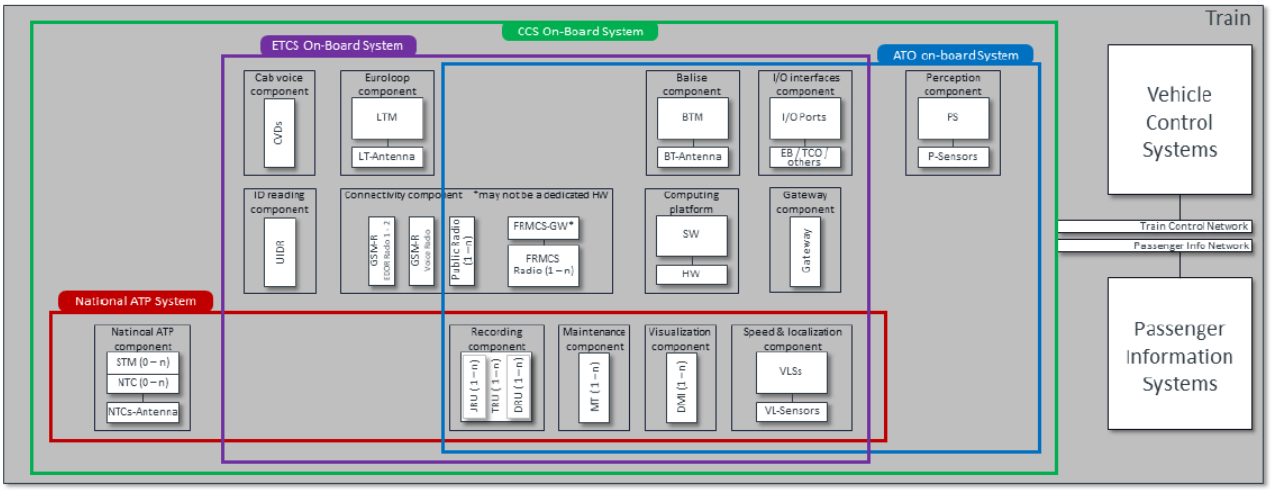

Figure 15 CCS On-board Subsystems Overview

The exact system boundary definition for the SuC will be defined in CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22]. Component and subsystem definitions will be available in CENELEC phase 5 – Architecture and Apportionment (CP5) according to EN 50126-1 [22].

Figure 16 shows an attempt to locate the SuC in the nesting of the different safety cases (SC).

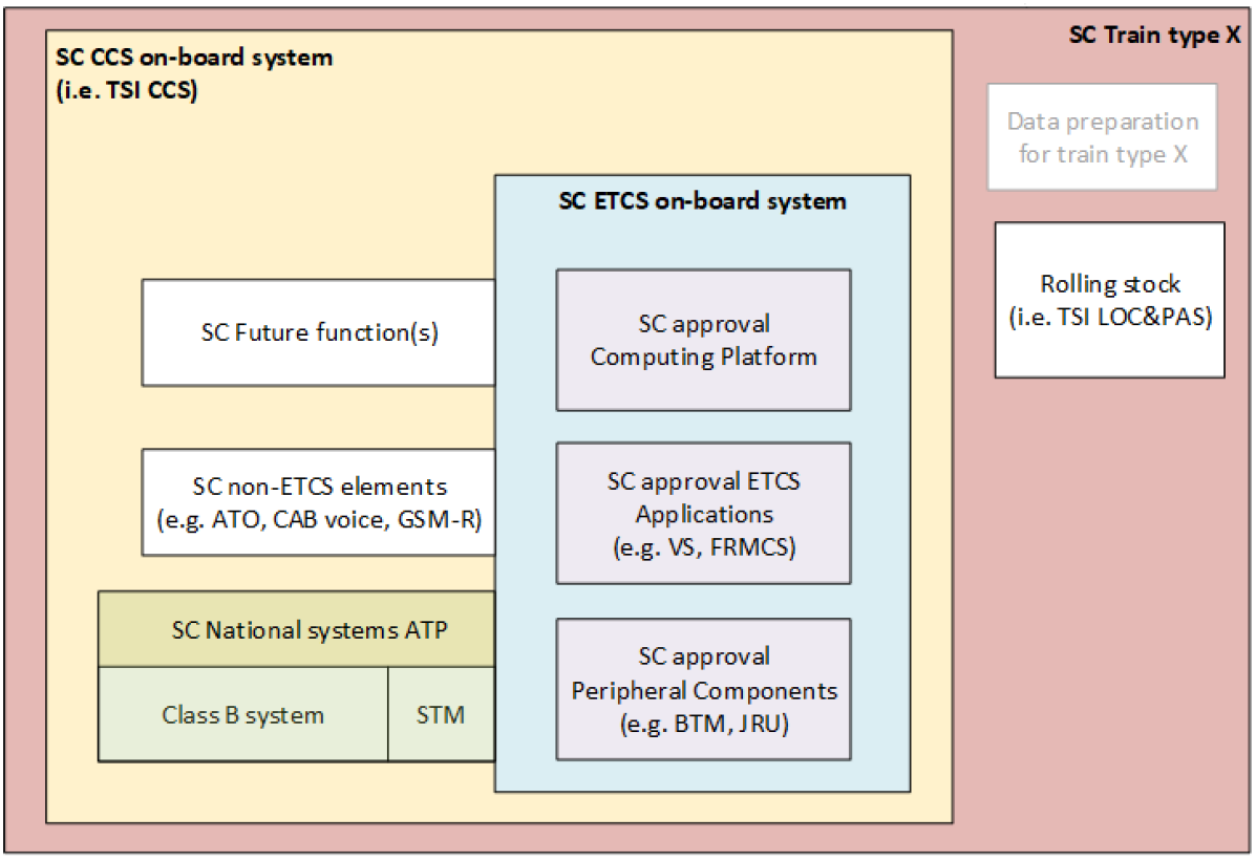

Figure 16 CCS on-board safety case nesting

Other systems like train control management systems (TCMS, Vehicle Control System) or passenger information systems are not in the scope of the system.

The nesting and safety case structure will be defined and explained in detailed in the OCORA Safety Plan during CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22].

In the following subchapters the development tasks defined by OCORA are described.

3.2.1 Task 1: Provide ETCS on-board functions

The CCS on-board system incorporates the ETCS on-board sub-system that provides all ETCS functions required on the vehicle. The typical core function is speed supervision for the evaluated location. Moving authority observation is basically performed on speed supervision combined with location information. The speed limit is evaluated based on the selected 'MODE', 'LEVEL' and information received from the trackside signalling system. To fulfill these core functions several auxiliary functions are required like vehicle speed evaluation, Balise information reading, radio messages processing, driver information acquisition and display, vehicle position determination, etc. The function and behaviour for ETCS is standardised at European level in specifications. The TSI Command Control and Signalling (CCS) provides a list of mandatory specifications for ERTMS, the CCS on-board system is included in this set of specifications.

3.2.2 Task 2: Provide ATO vehicle (on-board) functions

The CCS on-board system incorporates the ATO vehicle sub-system that provides all ATO functions required on the vehicle. The typical core functions are precise timetable execution (static and dynamic) by control of vehicle speed (decision for acceleration, deceleration, coasting, or constant speed) and precise vehicle stopping. ATO would also control the doors (GoA level 4).

3.2.3 Task 3: Provide cabin voice radio functions for the vehicle driver

The CCS on-board system incorporates all functions required for the voice communication from the vehicle driver to other people via radio. The communication to other people is required for operational reasons. This can be for instance personnel in the off-board control room or the train attendant. For the vehicle driver it shall be possible to select which connection he needs to establish. It shall also be possible to make calls from outside to the vehicle driver.

3.2.4 Task 4: Provide logic for synchronization of active ATP system

The CCS on-board system incorporates a logic (ATP Manager) that synchronizes the on-board ATP systems to the system that is available from infrastructure side. A specific track is typically equipped with an ATP system, sometimes with two in parallel. The vehicle needs to be equipped with the corresponding ATP system to safely run on the specific track. When a vehicle is equipped with more than one on-board ATP system, the on-board logic (ATP Manager) must activate the on-board ATP system that is compatible to the ATP system installed on the track. In addition, the logic (ATP Manager) synchronizes the different on-board ATP systems installed on the specific vehicle between each other. Depending on the requests from infrastructure side the on-board ATP systems are put to 'cold standby', 'hot standby', 'active', etc. There can be different on-board ATP systems for instance ETCS or the national systems (e.g., ATB in the Netherlands, LZB / PZB in Germany and Austria).

3.2.5 Task 5: Provide national ATP system functions

The CCS on-board system incorporates the national ATP on-board sub-system that provides all national ATP functions required on the vehicle. The typical core function is vehicle supervision. However, there are several different national ATP systems that work differently from each other and facilitate varying level of assistance. To provide functionality for national ATP system is optional. Depending on which tracks a specific train shall run, the train owner decides which national ATP system to install, if any.

3.2.6 Task 6: The System shall be based on a more modular architecture

The CCS on-board system shall be based on a more standardized architecture compared to the systems currently deployed on the vehicles.

The main goals of the standardization are:

- Introduce a more modular architecture with defined sub-systems, components, and interfaces. The intention is to define the components and their interfaces in such a way that these are replaceable (i.e., plug and play) with products from different suppliers.
- Open the market for suppliers of single components. In the long term this should lead to lower prices and allow to tackle obsolescence issues more efficiently.
- Have functionally well-defined components allowing to tackle upgrade issues that are easier to handle from a certification and homologation perspective.

The CCS on-board system shall be designed with a modular architecture supporting modular safety certification and modular homologation concept for the vehicle. Also, the principles of “low complexity” and “loosely coupled” should be applied to the system architecture. This will lead to more IT/OT resilience and will result in a higher (achievable) level of cybersecurity.

3.3 Purpose of the SuC

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., to enable of 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).

Current on-board architecture falls short of ensuring a sustainable market model allowing for a controlled (cost, performance, risk, planning) implementation of ERTMS throughout Europe.

The primary interoperability driver is rolling stock, not infrastructure, since rolling stock must be able to seamlessly access all ERTMS compliant infrastructure.

Due to the defined key principles in chapter 2.3 the new developed system design will seriously improve compared to the currently available solutions in terms of all RAM aspects.

From functional view the defined key principles like modularity will reduce the cost of functions, by reducing the umbers of units per train.

From operational view, the defined key principles like modularity, independence and plug and play exchangeability will affect the most and an RU will benefit during the life cycle, in terms of operation and maintenance (e.g., mean time to repair) and due to the reduction of follow-on certification efforts.

3.4 Environment of the SuC

3.4.1 Physical Aspects

Some standardized equipment locations within a vehicle must be determined to define the environmental conditions of the CCS on-board system that is composed of different equipment. EN 50155 [26] already defines typical locations shown in Figure 17.

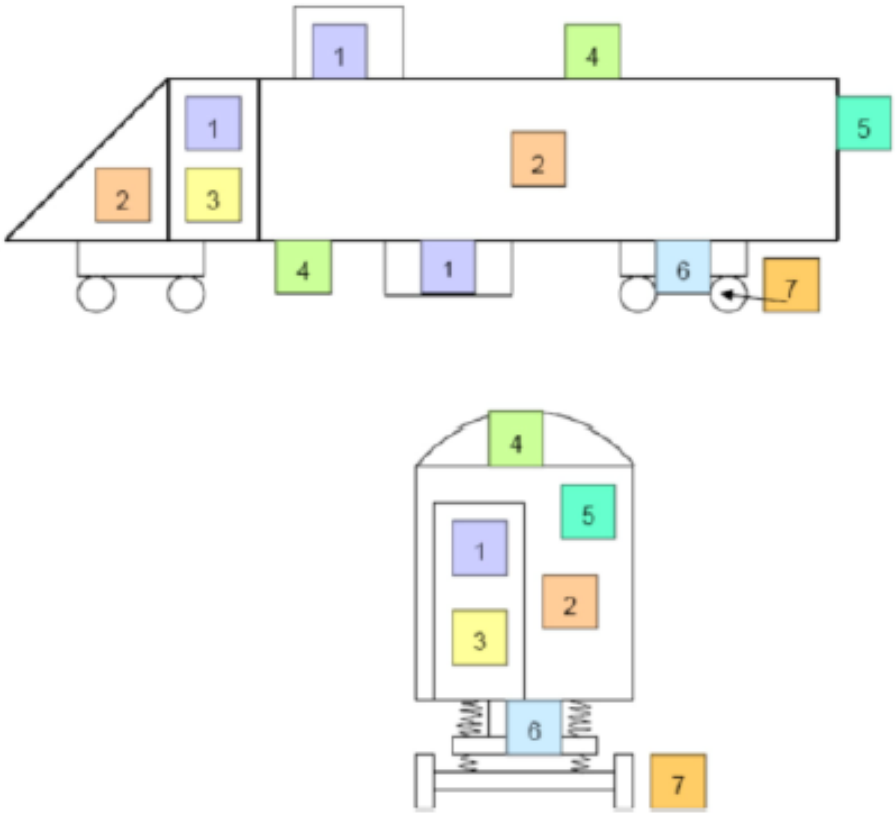

Figure 17 Typical equipment locations on board rolling stocks according to EN 50155 [26]

Each equipment location is detailed in the following table:

Location according to Figure 17	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 locations)	- 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 1 Example of typical equipment locations on board rolling stock according EN 50155

Separately for each equipment location the applicable environmental conditions are defined in this document.

Finally, it must be defined by the vehicle manufacturer in which equipment location a specific piece of equipment will be mounted.

Environmental conditions during operation:

Depending on the equipment location for each device of the CCS on-board system the environmental conditions according to the following table apply:

Environ-mental condition	Location 1	Location 2	Location 3	Location 4	Location 6	Location 7
Operating temperature (EN50155: 2017, § 4.3.2)	OT4	OT2	OT4	OT4	OT3	OT3
Extended operating temperature (EN50155: 2017, § 4.3.3)	ST1	ST1	ST1	ST1	ST0	ST1
Rapid temperature variations (EN50155: 2017, § 4.3.4)	H1	H1	H1	H2	H2	H2
Relative humidity (EN50155: 2017, § 4.3.7)	EN50125-1: §4.4 Humidity for TX	EN50125-1: §4.4 Humidity for T2	EN50125-1: §4.4 Humidity for TX	EN50125-1: §4.4 Humidity for TX	EN50125-1: §4.4 Humidity for T3	EN50125-1: §4.4 Humidity for T3
Shock and vibration (EN61373: 2010)	Category 1 Class B	Category 1 Class B	Category 1 Class B	Category 1 Class B	Category 2	Category 3
Wind (EN50125-1: 2014, § 4.5.1)	No specific requirement	No specific requirement	No specific requirement	No specific requirement	No specific requirement	No specific requirement

Environ-mental condition	Location 1	Location 2	Location 3	Location 4	Location 6	Location 7
Surrounding air (EN50125-1: 2014, § 4.5.2)	The pressure pulse will have to be provided later	No specific requirement	No specific requirement	The pressure pulse will have to be provided later	The pressure pulse will have to be provided later	The pressure pulse will have to be provided later
Rain (EN50125-1: 2014, § 4.6)	No specific requirement	No specific requirement	No specific requirement	Class 5K3 of EN 60721-3-5	Class 5K3 of EN 60721-3-5	Class 5K3 of EN 60721-3-5
Snow and hail (EN50125-1: 2014, § 4.7)	No specific requirement	No specific requirement	No specific requirement	S3	S3	S3
Ice (EN50125-1: 2014, § 4.8)	Analysis results to be provided	No specific requirement	Analysis results to be provided	Analysis results to be provided	Analysis results to be provided	Analysis results to be provided
Solar radiation (EN50125-1: 2014, § 4.9)	No specific requirement	No specific requirement	No specific requirement	5K2 or 5K3 of EN 60721-3-5 R2	5K2 or 5K3 of EN 60721-3-5 R1	5K2 or 5K3 of EN 60721-3-5 R2
Lightning (EN50125-1: 2014, § 4.10), indication based on EN50124-1: 2017	OV2	OV2	OV2	OV4	OV4	OV4
Pollution Degree (EN50124-1: 2017)	PD2	PD2	PD3	PD3	PD4	PD4
Pollution (EN50125-1: 2014, § 4.11), indication based on EN 60721-3-5	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2	chemically active substances Class 5C2 biologically active substances Class 5B2 dust defined by Class 5S2 grasses and leaves, pollen, flying insects, fibres etc. sand sea spray according to Class 5C2
Animals on track (EN50125-1: 2014, § 4.12)	No specific requirement	No specific requirement	No specific requirement	Hit with animals up to 800kg	Hit with animals up to 800kg	Hit with animals up to 800kg
Ingress protection degree (EN60529: 1999 + A2: 2013)	IP 20 or more stringent	IP 30 or more stringent	IP 20 or more stringent	IP 67 or more stringent	IP 67 or more stringent	IP 67 or more stringent
Resistance to light (UV)	No	No	No	Yes	Yes	Yes
Resistance to ozone for rubber and plastic parts	No	No	No	Yes	Yes	Yes
Operating temperature (EN50155: 2017, § 4.3.2)	OT4	OT2	OT4	OT4	OT3	OT3
Extended operating temperature (EN50155: 2017, § 4.3.3)	ST1	ST1	ST1	ST1	ST0	ST1

Table 2 Environmental conditions

Note: Equipment location 5 is not applicable, as the CCS on-board system equipment's cannot be mounted in this area. The values have been defined according to assumptions (see chapter 8.1.2).

This allocation of the OCORA constituents towards Figure 17 will be performed in CENELEC phase 2 - System Definition (CP2) from EN 50126-1 [22].

3.4.2 Interface Aspects

One of the main objectives of the OCORA project is to improve the modularity within the future CCS on-board systems. The overall vision of this is presented in Figure 6. Regarding the interfaces, the OCORA projects aims at defining:

- Standalone on-board constituents: modules realizing one or several ETCS functions,
- UVCCB: common bus used to interconnect the ETCS modules together,
- Vehicle adapter: standard gateway which interconnect the UVCCB to the existing train interfaces of the rolling stock

This vision is different from today's situation presented in SUBSET-026 for the ETCS on-board system. In the current version of the TSI CCS [29], the ETCS on-board system is defined as a monolithic block (see Figure 18) with proprietary interfaces between the different modules (e.g., BTM, TIU, KERNEL).

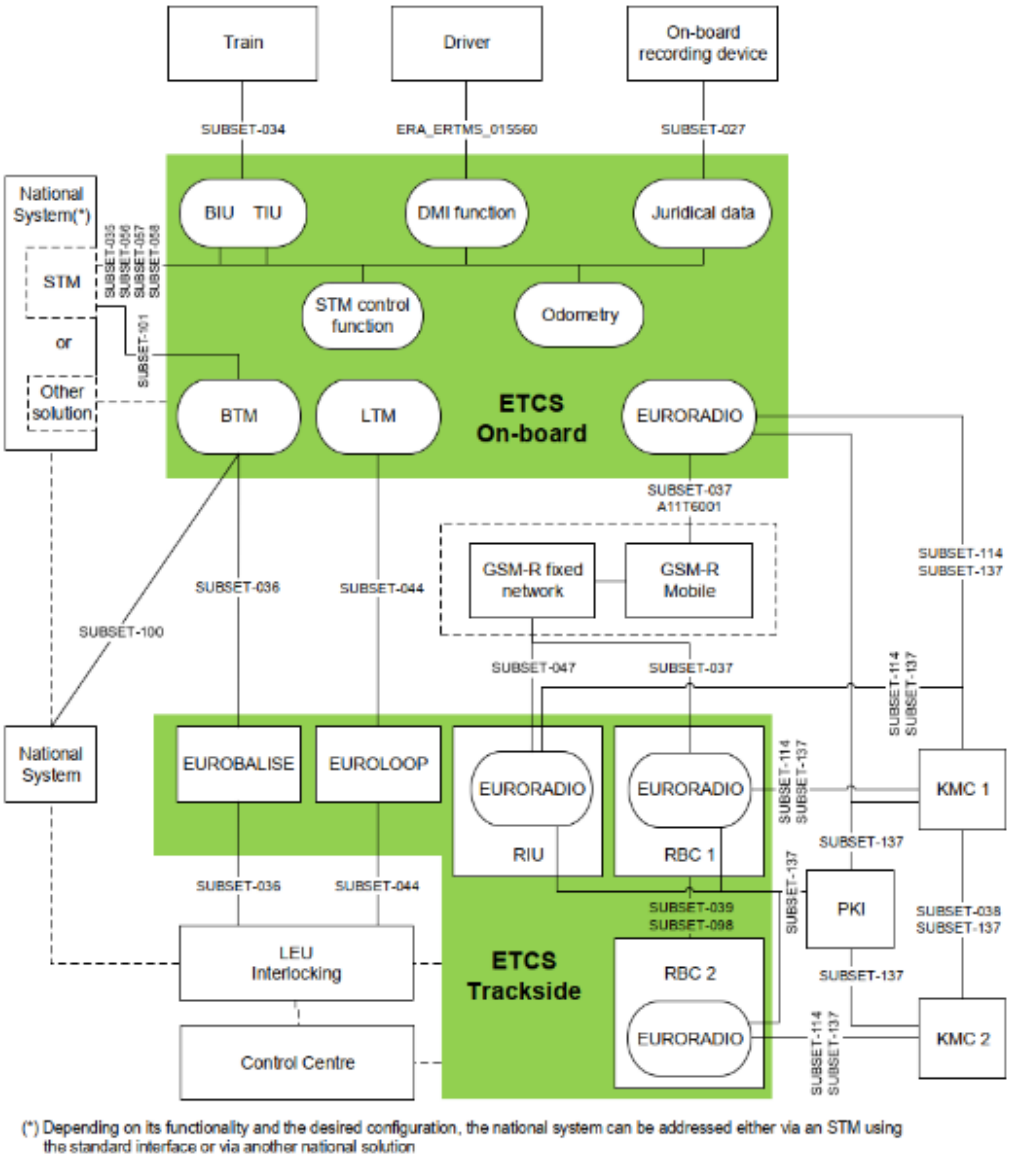

Figure 18 ERTMS/ETCS system and its interfaces

One of the main challenges of the OCORA project is to propose a standardized set of CCS on-board internal (i.e., between modules) and external (i.e., between OCORA and rolling stock, RCA, TOBA) interfaces.

This modularity stimulates the lifecycle management for the CCS on-board systems as it will ease its evolution without degrading the overall safety management as stated in the Modular Safety document [20].

4 Previous RAMSS Requirements of similar and/or related systems

4.1 RAM

The following reliability target values indicated have been defined by SBB for the "ETCS zweite Welle" project. The values are derived from the specification ETCS generic technical specification that was released 2012.

The reliability targets for the ETCS on-board system are defined as follows :

Incident class	Target value
Failure without direct effect on the operation but which requires a corrective action (incident class 0).	λ0 ≤ 0.73 per year
Failure that triggers the service brake, or the emergency brake, by which the train is brought to standstill. The train however can resume operation without limitation (incident class 1.i).	λ1 ≤ 0.15 per year
Failure or partial failure of the odometry sub-system, such that not all odometry data can be used for operation (incident class 1.ii).	λ1 ≤ 0.15 per year
Failure that triggers the service brake, or the emergency brake, and requires a system restart (“reset”) or a reconnection to the RBC. After being brought to standstill and having restarted the system, or established again connection to the RBC, the train can resume operation without limitation (incident class 2).	λ2 ≤ 0.050 per year
Failure that prevents operation in ETCS Level 2 Full Supervision, by which however the operation in ETCS Level 0 and use of all in the vehicle installed Class B systems is possible without restriction (incident class 3a).	λ3a + λ3b ≤ 0.050 per year
Failure that prevents operation in either ETCS Level 2 Full Supervision or with at least one in the vehicle installed Class B systems (incident class 3b). class	λ3a + λ3b ≤ 0.050 per year

Table 3 Previous Reliability Target of SBB Call for Tender

The following maintenance target values are derived from the ETCS generic technical specification for the "ETCS zweite Welle" project by SBB that was released in 2012.

The diagnosis system must achieve the following targets:

- 21/114 Rev: 563388
- First year from delivery: NFF (“No Fault Found”) =20%
- 2nd year from delivery: NFF=15%
- 3rd year from delivery: NFF=10%

The mean preventive maintenance time shall not exceed 6 hours per year. For calibration activities, the duration from the moment where the measurement is available, to the moment the vehicle is available for operation, shall not exceed 15 minutes. The complete software and parameter installation (including the software verification and test) shall not exceed 60 minutes.

The document “RAM_concept_3rd_wave” from the SBB also reports the following risks:

Software risk:

- Many, serious software errors at delivery.
- Too few opportunities to correct these or have them rectified timely.
- Another problem is the introduction of software errors with new software versions.
- Possible consequence: delay and loss of mission, many train cancellations.

Risks during integration into the vehicle:

- Integration of two disciplines (vehicle system engineering, signalling technology) with their different cultures and ways of thinking.
- Possible consequence: unsuitable integration has a negative impact on reliability and availability.
- This risk can be mitigated by ensuring an accurate integration and a working continuous performance monitoring.

Critical individual components (DMI, Eurobalise antenna and EVC):

One of the critical components DMI / Eurobalise antenna does not reach the required performance. Possible consequence: many delays and train cancellations.

Note: the EVC (computer) is listed as critical component due to its significance. Its incident rate in current systems is however not attracting attention.

Odometry:

Insufficient odometry performance leads sometimes to comprehensive delays. This risk persists especially on days with demanding (but by no means exceptional) weather conditions, especially with snow.

European level, the feedback for ETCS on-board systems performance is described in the OCORA Architecture Alpha chapters 1.2, 1.5 and referenced document. It is reported that the operational reliability, availability, and maintainability performance values plus the costs of deployed ETCS on-board systems have not reached a satisfying level.

4.2 Safety

Within the OCORA project, the architecture of the CCS on-board system is being developed further with a holistic approach. This has an impact also on the incorporated ETCS on-board sub-system that will replace the system available on today's market also called EVC (European Vital Computer). The latter is described in SUBSET-026 [31] from a functional point of view and in SUBSET-091 [32]regarding safety related hazards. The following functional figure of the ETCS on-board system is extracted from SUBSET-091 v3.6.0 [31]. It presents all the recognised hazardous events to be managed in the Hazard Log when developing an interoperable EVC compliant with TSI CCS [29]. This "ETCS on-board solution" presents the functional basis for the future OCORA compliant ETCS on-board system.

Within the OCORA project, further functions are added to the CCS on-board system, which results in new sub-systems in addition to today's "EVC" scope (e.g., ATO, FRMCS). Unfortunately, SUBSET-091 [32] is not yet in line with this new functional scope. The harmonisation will be done in 2022 with the new release of the TSI CCS [29]. Therefore, the current safety targets coming from SUBSET-091 [32] must be taken as input for the first release of the safety risks analysis.

In this context, all the hazardous events documented in SUBSET-091 [32] (see Figure 19) are applicable to the OCORA project. Later, in CENELEC phase 3, these will be used as basis to perform the risk analysis.

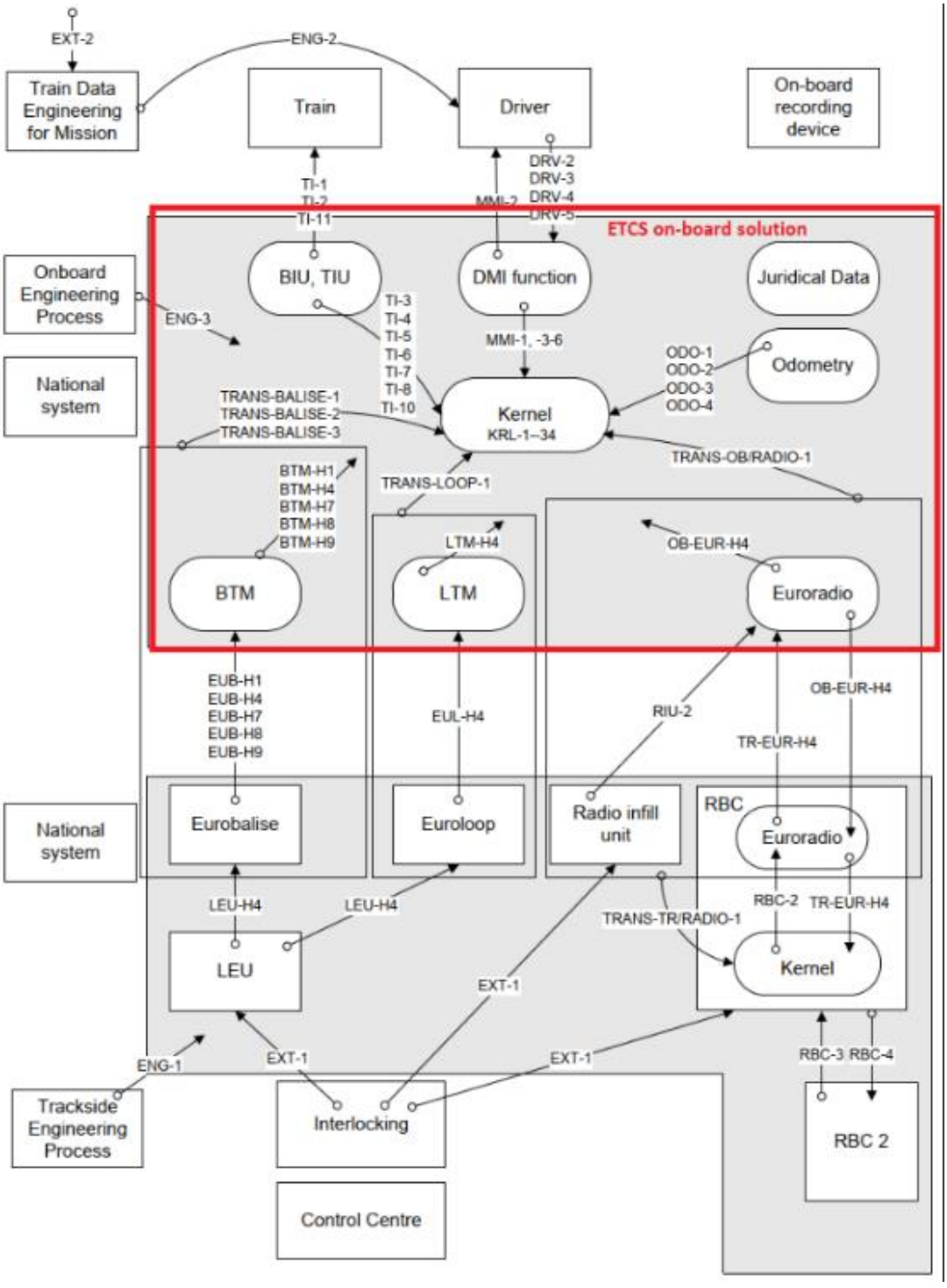

Figure 19 Graphical representation (from SUBSET-91) of the hazardous events within the ERTMS/ETCS Reference Architecture adapted for THR allocation

4.3 Security

The primary goal of security in connection with security-relevant systems or applications is to ensure that security incidents have no impact in safety incidents and stable operation is guaranteed. To guarantee undisturbed railway operations, it is necessary to implement preventive protection against cyber-attacks. By developing security solutions, the goal is to achieve a layering of safety and security. There are dependencies and according to TS 50701 [28] it is necessary to separate the security development from the safety development as far as possible. Therefore, security updates do not require a new safety certification.

The whole ERTMS system has grown in time and in technology. It is a patchwork with spreading of many elements over the EU and with interfaces and relations to neighbouring countries. The high number of interfaces and interdependencies pose a high risk for cross company infections and incidents. Old analogue systems, electronic interlocking and digital control are all existing beside each other. Since security always depends on the weakest element in the chain, the vulnerabilities are manifold. With the actual strongly increased cyber vector for attacks and the simple possibilities in organizing vandalism over social channels, the rail system has become very vulnerable to intentionally motivated attacks.

Architectural deficits on trains

Trains are nowadays rolling data centres. Data centres need a high level of architectural protection measures Both on physical as well as on software and architectural levels (e.g., network design principles). On trains we have today only very few segregations of networks and services. The co-existence of passenger services like Wi-Fi, public screens, passenger information and train control elements, pose a risk of hopping and lateral movement attacks. Not only targeted attacking but also electronic vandalism must be prevented from. Modern trains are much higher exposed to it than older trains because of the increased attack vector of cyber and local attacks.

In general, poor physical security on trains

Another critical gap is the physical security of locomotives. Locomotives and train compositions are sometimes left unlocked. Apart from this, it is currently also possible to use the simplest means to gain unauthorized access to a driver's cabin or the cabinets with electronic hardware. A state-of-the-art, future proof IAM concept, which ensures access even when the vehicle is disconnected, must be implemented.

Interoperability of the trains

Another aspect that needs to be clarified at an international level is the interoperability of the trains. Even when crossing a border, it must be ensured that all essential security and safety functions are fully guaranteed.

Confidentiality of data on trains, missing basic communication confidentiality

Since old protocols are used even on new trains, communication can easily be listened to, analysed, manipulated, or interrupted. Even though the content is not a very confidential information itself, but the simple possibilities to analyse it and the poor integrity checks and controls pose a high risk of manipulation. When signals cannot be trusted, also safety functions with good concepts are worthless. Safety starts with security and security. And the whole chain of attack starts always with information gathering. Only confidentiality and encrypted information interrupts this attack vector from beginning. Here we have a gap that must be filled.

In general, poor security level in almost all disciplines on trains

Even old trains pose a quite high risk of weak protection against intentional attacks. It is easy to access a train driver cabin and start driving. Newer trains do not have much higher measures against intentional misuse but have a much higher potential in cyber security and physical/technical combined attacks. A modern train is a rolling data centre. In data centres we apply high standards for security. On a train, they are low. It starts with broadly available information on the internet continues in very poor physical security and ends up in old technologies in communication, authentication, and access management. Intentional attacks could interrupt or damage safe operation significantly.

5 Past RAMS Performance of similar and/or related Systems

Performance of operating ETCS on-board systems at SBB, the performance of operating ETCS on-board systems has been analysed in the RAM_concept_3rd_wave. The RAM performance of 293 ETCS on-board systems has been monitored for 18 months. It is summarized per OBU per year as follows:

Count: Intrinsic failure	Count: train outage after an internal failure	Count: train outage after failure of another train	Passenger delay minutes	Corrective maintenance cost (hardware and staff)
3.4	0.16	0.35	8'300	CHF 4'400

Table 4 Performance of Operating Systems

6 Current RAMSS Policy and Targets of the relevant Railway Duty Holders

6.1 RAM

In order to ensure a sufficient RAM performance of the overall CCS and its subsystems, the following principles are pursued with the RAM policy:

- Definition of definite and verifiable RAM targets for the overall system and its RAM-relevant subsystems
- Development in accordance with the prescribed laws and standards
- Conduct of the life cycle according to the EN 50126-1 [22] standard for the overall CCS and its RAM-relevant subsystems
- Definition of methods and procedures for each life cycle phase that are suitable to perform the planned activities for each phase
- Proof of the successful run of the lifecycle or parts thereof in a RAM proof for the overall CCS and its RAM-relevant subsystems
- Verification of the phases' activities and results
- Validation of definition and fulfillment of the requirements
- Realization of the OCORA specification on quality, configuration and change management

The extent and depth of the RAM process, which will be applied for subsystems according to EN 50126-1 [22], is still under clarification. The implementing provisions for the railway ordinance stipulate that for all telematics applications directly involved in railway operations (e.g. control and automation technology) and which are directly related to the safety and reliability of railway operations, the CENELEC standard to EN 50126-1 [22]must be applied for the specification and proof of fulfilment of the reliability, availability, maintainability, and safety requirements (RAMS requirements). Outside the scope of the CENELEC standard to EN 50126-1 [22] are e.g. applications, which serve the planning or disposition of railway operations.

Superordinate availability targets to overall system and subsystems are formulated and quantified as train delay minutes caused by the respective (sub)systems. These consider passenger and freight traffic and include primary as well as secondary delays. For availability, only corrective maintenance is considered; preventive maintenance is a scheduled activity and does not influence the availability calculation.

The RAM management subordinates to the OCORA process and will be treated in more detail in the OCORA RAM Plan during CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [22].

6.2 Safety

OCORA project will mostly rely on the existing safety analyses performed during for the TSI CCS (2016 release and before). Indeed, the largest part of the risk assessment analysis and evaluation (i.e., CENELEC Phase 3) regarding the existing CCS on-board functions (e.g., BTM, I/O Ports, VS application) is already covered in the safety subset (e.g., 088, 091, 120) and will not evolve.

The new game changer ATO (GoA1/2) that will be introduced in the TSI CCS 2022 should be stated as not safety related. Thus, the focus of the risk assessment strategy for OCORA will be on the new CCS functionalities such as VIAM and DCM are defined in OCORA architecture. Likely, these new functions could be linked to existing hazards identified in Subset-088.

Furthermore, OCORA initiative is composed of different European RU members but has no legal frame. Each company has its own Safety Policy based on technical and political choices. In that context, the definition of a common Safety Policy for OCORA would be a very difficult task for a very limited or even maybe no usage.

Therefore, it is decided to not define an OCORA Safety Policy at this step of development and wait for the Phase 3 investigations to state if it becomes a necessity for the project or not.

6.3 Security

There are two kinds of threats resulting from unauthorized access to signalling equipment:

- Physical security threats
  It is established good practice to protect systems from direct access to signalling equipment, which could allow unauthorized persons to cause (intentionally or unintentionally) functional safety hazards.
- IT-Security threats
  Modern IT communication concepts result in the need to protect those systems also against logical access via IT systems.

IT-Security is a rapidly evolving field. IT-Security can affect not only the service but also functional safety of a signalling system. However, there is no inherent relationship between security and safety requirements. Several standards exist which give detailed advice on how to deal with IT-Security threats. These standards are also valuable, considering impacts on functional safety, which are simply additional effects of threats generally regarding IT-Security.

This document does not specify the requirements for the development, implementation, maintenance and/or operation of security policies, security services or security systems, for which appropriate IT-Security standards are applicable.

IT-Security threats shall be managed during the Risk Assessment and Hazard Control (or existing analyses shall be referenced), if an impact of IT-Security issues on functional safety is reasonably foreseeable and cannot be excluded by simple arguments (e.g., a system having no connection to untrusted networks). Measures addressing security shall be recorded or referenced in the Safety Case (section 4.5 of the Technical Safety Report).

IEC/ISO standards that address IT-Security in depth are ISO 27000ff, ISO/IEC/TR 19791, and the IEC 62443 series. Measures used to achieve a certain SIL will not necessarily ensure security and, on the other side, the concept of SIL is not intended to be applied to IT-Security requirements. Typical consideration of security versus safety is the need for fast security updates of SW arising from security threats, whereas if such SW is safety-related, it is thoroughly developed, tested, validated, and approved before any update. Like systematic errors, probabilistic evaluation of IT-Security threats is considered infeasible. Requirements for safety-related data communication, given in EN 50159 [27], cover some aspects of IT-Security.

OCORA Cybersecurity has already an alinement with the other initiatives like the EULYNX security cluster in these terms.

Please refer to the OCORA Project Security Management Plan for more details about the defined targets (standard, risk assessment, etc.).

7 Safety Legislation

7.1 European Legislation

The CCS on-board system is defined according to TSI CCS [29] which requires a set of standards and technical specifications as mandatory. The structure is shown in the figure below:

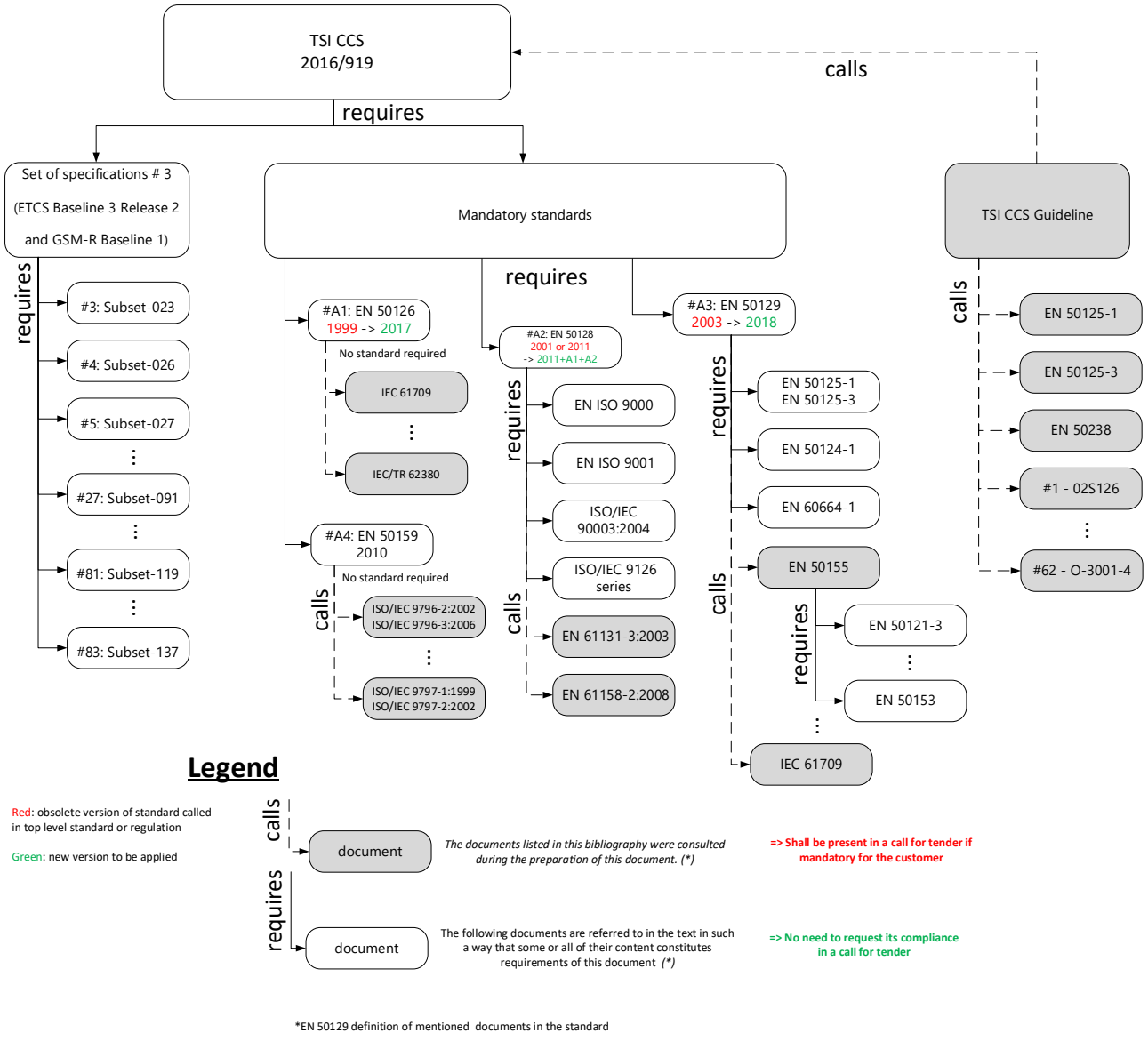

Figure 20 TSI CCS regulations content

In addition, the TSI CCS [29], mentions other documentation as optional. They will be used for the OCORA project development.

It concerns:

- EN 50155 [26]
- TSI guideline GUI/CCS TSI/2019 [29] for the methodology and the following documentation:
    - EN 50125-1
    - EN 50125-3
    - EN 50238
    - #1 - 02S126
    - #2 - 97S066
    - #3 - SUBSET-074-1
    - #4 - 97E267
    - #9 - ERA/ERTMS/040092
    - #16 - ERA/ERTMS/040093
    - #40 - ERA/ERTMS/040063
    - #47 - SUBSET-113
    - #49A – EN 50592
    - #54 - SUBSET-119

7.2 ERTMS national Rules

The OCORA project aims to be a unified common vision for future CCS on-board systems. Therefore, the consideration of all NNTR from all European countries into the project is impossible and not relevant.

Nevertheless, the OCORA project considers them by always leaving the possibility, through adapters (i.e., HW and/or SW) to connect the legacy STM systems to the future CCS on-board systems. For that, the analysis of STM related SUBSETs is in the scope of the OCORA project. It concerns:

- SUBSET-056: STM FFFIS Safe time layer
- SUBSET-056: STM FFFIS Safe link layer
- SUBSET-102: Test specification for interface "K"
- *SUBSET-074-1: Methodology for testing FFFIS STM
- SUBSET-074-2: FFFIS STM Test cases document
- *SUBSET-074-3: FFFIS STM Test specification traceability of test cases with specific transmission module FFFIS
- *SUBSET-074-4: FFFIS STM Test specification traceability of testing the packets specified in the FFFIS STM application layer
- SUBSET-101: Interface "K" Specification
- SUBSET-100: Interface "G" Specification
- SUBSET-059: Performance requirements for STM
- SUBSET-058: FFFIS STM Application layer

*These documents are called in the TSI Guideline [30] (i.e., optional) and not directly in the TSI CCS [29] (i.e., mandatory).

The OCORA design should leave the possibility to include NR; but will not include them inside the reference architecture. So, OCORA will not define a solution for a specific country, it needs to be adapted for each project/country solution.

The European Union Agency for Railways (ERA) document “ETCS and GSM-R national technical rules” gives an overview and provides all the relevant weblinks to the different national rules. According to its ‘rules cleaning-up programme’, ERA examines the existing national rules in the Member States to ensure that only allowed national rules are applicable. ERA is developing the Single Rules Database (SRD) that will replace the above registers. The SRD will be the unique tool for the notification of all draft national rules and all existing national rules.

8 Assumptions and Justifications

Any Assumptions or justifications made during the first life cycle phase is documented in this chapter.

8.1 Assumptions

8.1.1 No Interface to EULYNX

Based on the review of the EULYNX documentation (e.g., System Definition) no interfaces to OCORA were discovered.

8.1.2 Equipment Location

Equipment location 5 is not applicable, as the CCS on-board system equipment's cannot be mounted in this area. The values have been defined according to assumptions

8.1.3 Harmonised OCORA RAMS Policy and Targets

OCORA defined its own RAMS policy, targets, and performances based on information provided by SBB.

8.1.4 OCORA Deliveries

OCORA identified and defined documents from CENELEC phase 1 to 5 that will be produced and decided which of them are being published.

8.2 Justifications

8.2.1 RCA Dependency

The dependency between OCORA and RCA was analysed. OCORA defines an independent system but considers and implements the results and specifications especially related to the system interfaces provided by RCA.

9 Open Issues

None

End of document