OCORA

Open CCS On-board Reference Architecture

Design Requirements

Document ID: OCORA-TWS01-010

Version: 2.0

Release: R1

Date: 26.11.2021

Revision History

Version	Change Description	Initials	Date of change
1.01	Official version for OCORA Delta Release	TM/AL	30.06.2021
2.0	Official version for OCORA Release R1	TM/AL	26.11.2021

Table of Contents

References

Reader's note: please be aware that the document ids in square brackets, e.g. [OCORA-BWS01-010], as per the list of referenced documents below, are used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always references to the latest available official version of the SUBSET, unless indicated differently.

[OCORA-BWS01-010] – Release Notes
[OCORA-BWS01-020] – Glossary
[OCORA-BWS01-030] – Question and Answers
[OCORA-BWS01-040] – Feedback Form
[OCORA-BWS03-010] - Introduction to OCORA
[OCORA-BWS03-020] - Guiding Principles
[OCORA-BWS04-010] - Problem Statements
[OCORA-TWS05-020] – Stakeholder Requirements
[OCORA-TWS05-021] – Program Requirements
[OCORA-BWS07-010] - Alliances

1 Introduction

1.1 Purpose of the document

The purpose of this document is to provide a collection of all Design Requirements (B-Level requirements) in a structured manner. Please be aware of the Stakeholder Requirements (A-Level requirements) provided in [OCORA-TWS05-020]. Also note that Program Requirements are not covered in this document as they are covered in a [OCORA-TWS05-021] .

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [OCORA-BWS01-040] .

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 organisation interested in developing CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

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

1.3 Context of the document

This document is published as part of the OCORA Release R1, together with the documents listed in the release notes [OCORA-BWS01-010] . Before reading this document, it is recommended to read the Release Notes [OCORA-BWS01-010]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [OCORA-BWS03-010], and the Problem Statements [OCORA-BWS04-010]. The reader should also be aware of the Glossary [OCORA-BWS01-020] and the Question and Answers [OCORA-BWS01-030].

1.4 Requirements Engineering Process

This OCORA requirement document is developed, using the Requirements Management Guideline [OCORA-TWS05-010]. The requirements are engineered in a top-down manner:

- As a starting point all **"Stakeholder Requirements"** towards the OCORA initiative **(A-Level requirements)** are captured and formalised.

- In a second step, the **"Program- and Design Requirements" (B-Level requirements)** are developed. These requirements define tools, processes, methodologies and design rules to be used within the program and to be considered during the system analysis and the system design/architecture work.

- As a next step, the A- and B-Level requirements are further developed in the MBSE analysis to become **"System Requirements" (C-Level requirements).**

- As part of the MBSE architecture work, building blocks are identified taking into account the MBSE analysis (C-Level requirements). All applicable requirements (A-Level, B-Level, and C-Level) are apportioned to the identified building blocks, resulting in **"Building Block Requirements" (D-Level requirements)**, forming the OCORA tender templates, together with the applicable program & design requirements.

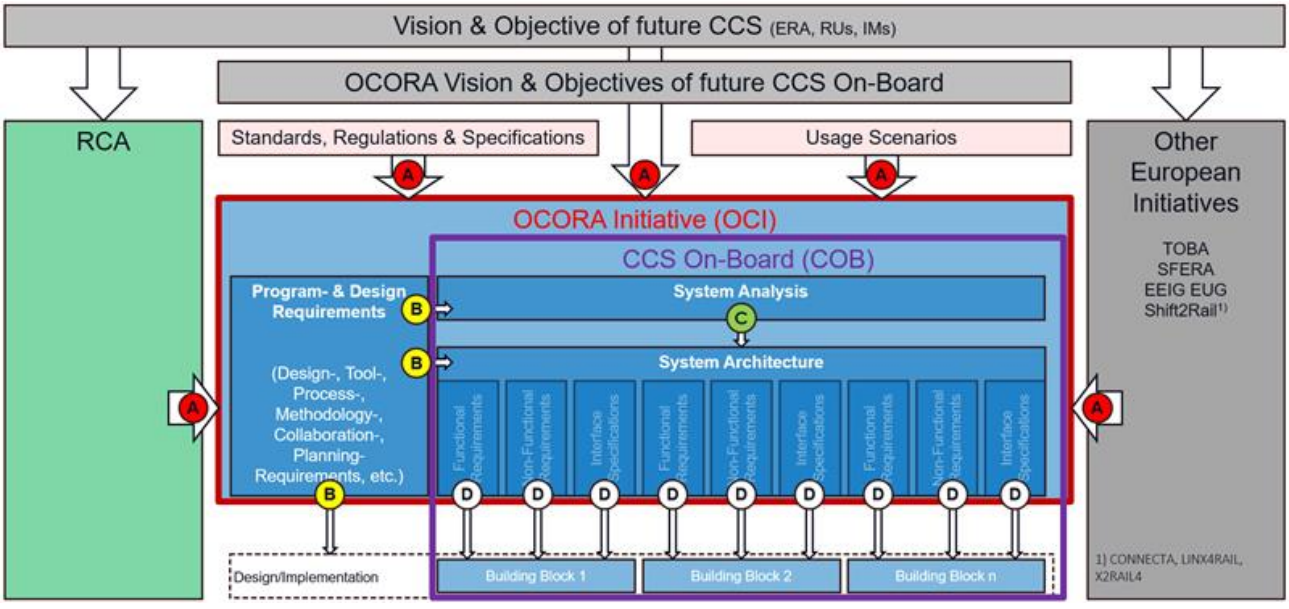

Figure 1 OCORA Requirements Engineering Process

Please note, that the A-Level requirements are applicable to the OCORA Initiative (OCI) while the B- and C-Level requirements are targeted towards the CCS On-Board System (COB) and its architecture. D-Level requirements are applicable to the respective building blocks.

2 Architectural process requirements

2.1 System decomposition principles

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 [OCORA-BWS03-010].

The term OCORA building block is used in the following requirements. In order to provide the reader with a better understanding, the definition of an OCORA building block is quoted below:

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".*

OCORA-544, B-Level - Aim for reasonable decomposition granularity

The system decomposition into building blocks is be based on the lowest reasonable granularity.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To enable the maximum level of value for money
Verification Method	Design Review

OCORA-545, B-Level - Use narrow interfaces

Building blocks have narrow, well defined standardised interfaces.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve low coupling. • Narrow Interfaces are easier to extend, maintain, reimplement • Few operations and limited functionality is easier to maintain and less error prone
Verification Method	Design Review

OCORA-546, B-Level - Ensure regression-free testing

Building blocks allow for regression-free testing. This means that changes done to a building block will only require testing of this building block and no regression testing of all test cases where the respective building block is involved.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To minimize the testing effort.
Verification Method	Design Review

OCORA-547, B-Level - Avoid mixing functions of different quality attributes

Aim for a strict separation of functions with different quality attributes (safety, availability, performance).

Status	✓ Approved
Req. Class	Requirement
Rationale	• Since the function requiring the highest quality attribute defines the quality required of all other functions in the same building block, mixing of functions requiring different quality attributes in one building block shall be prevented.
Verification Method	Design Review

OCORA-548, B-Level - Isolate deprecated functions

Functions not needed in the future (e.g. GSM-R), are isolated.

Status	✓ Approved
Req. Class	Requirement
Rationale	• This allows easy removal, once the functionality is not needed anymore.
Verification Method	Design Review

OCORA-549, B-Level - Consider installation locations

It is considered that physical distribution of building blocks / components over the train is needed in some cases (e.g. antenna positioning, etc.)

Status	✓ Approved
Req. Class	Requirement
Rationale	• To minimize installation efforts • To ensure the solution is fit for purpose
Verification Method	Design Review

OCORA-550, B-Level - Isolate optional functions

Functionality not needed in all CCS on-board implementations is isolated into separate building blocks or components.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To allow deployment of functionality on an as needed basis
Verification Method	Design Review

OCORA-551, B-Level - Ensure coherent and consistent life-cycles

Functional decomposition and functional allocation ensure coherent and consistent building block life-cycles.

Status	✓ Approved
Req. Class	Requirement
Rationale	• This is to achieve an independent life-cycle management for each of the building blocks. • This concerns especially 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).
Verification Method	Process Review

OCORA-566, B-Level - Favor off-the-shelf products

OCORA considers off-the-shelf products whenever reasonably possible.

Status	✔ Approved
Req. Class	Requirement
Rationale	• To minimize cost • To minimize hardware components needed • To improve life-cycle maintenance
Verification Method	Process Review

2.2 Architectural design guidelines

The OCORA architecture design principles formulated in document [OCORA-BWS03-010] can be operationalised into the system architecture design guidelines.

OCORA-552, B-Level - Aim at realizing functions in software

Aim at realising functions in software (applications and services) and avoid binding them to a specific hardware.

Status	✔ Approved
Req. Class	Requirement
Rationale	• To maximize reuse. • To protect investments. • To improve expandability • To facilitate innovation
Verification Method	Process Review

OCORA-554, B-Level - Strive for a modular software design

Software components can be updated, upgraded, removed, added, or exchanged without the need for hardware changes or (re)certification of other than the software affected.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To protect investments. • To minimize certification effort. • To respect different life-cycles.
Verification Method	Design Review

OCORA-553, B-Level - Isolate Core ETCS functionality

Core ETCS functionality is isolated from other on-board functions.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To respect different life-cycles • To make it reusable for different deployment scenarios (considering development, certification, etc.)
Verification Method	Design Review

OCORA-555, B-Level - Standardise interface to the Physical Train Unit

OCORA aims to standardise the interface to the physical train unit.

Status	✓ Approved
Req. Class	Requirement
Rationale	• Prerequisite for reusing the same CCS on-board system for multiple vehicles • To respect different life-cycles
Verification Method	Design Review

OCORA-557, B-Level - Consider open standards whenever possible

Open standards are used whenever reasonably possible.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To make building blocks more functional and interoperable • To streamline product development • To avoid vendor-imposed boundaries
Verification Method	Process Review

OCORA-558, B-Level - Maximize software re-use

Software components are architected and designed to allow for re-use in different deployment scenarios.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To maximize software quality • To minimize test and certification efforts
Verification Method	Design Review

OCORA-559, B-Level - Avoid code duplication

Whenever reasonably possible, common functionality is isolated and re-used by different applications.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To maximize software quality
Verification Method	Design Review

OCORA-560, B-Level - Promote automated testing

OCORA promotes automated testing and provides the enabling design and technology.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To minimize the test effort • To have a wider test coverage • To ensure consistency • To ensure replicability • To increase efficiency
Verification Method	Design Review

OCORA-561, B-Level - Aim for balanced integration effort

OCORA strives for a balanced relation between modularity and integration effort.

Status	✓ Approved
Req. Class	Requirement
Rationale	• Ensures that modularity benefits are not sacrificed by exponential integration effort.
Verification Method	Design Review

OCORA-562, B-Level - Aim for a strict separation of hardware and software

Whenever reasonably possible, OCORA aims to strictly separate hardware and software (business logic).

Status	✓ Approved
Req. Class	Requirement
Rationale	• To be able to handle the very different life-cycles. • To protect the investment of developed software. • To maintain software quality across different hardware generations.
Verification Method	Design Review

OCORA-563, B-Level - Promote competitive building block market

OCORA aims for a healthy, competitive building block market.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To improve quality. • To improve price. • To avoid vendor lock-in. • To ensure vendors are interested in supplying building blocks
Verification Method	Process Review

3 Architectural infrastructure requirements

3.1 Communication Requirements

3.1.1 On-board communication

Today the interfaces between CCS components on the vehicle are proprietary. The proprietary interfaces do not allow to exchange or update CCS components from different suppliers. The OCORA aims for plug and play like interchangeability within the CCS domain through the specification of a generic and open communication backbone.

OCORA-169, B-Level - Standardised Common Communication Infrastructure

All building blocks communicate through a specified and standardised common communication infrastructure.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability. • To reduce overall integration complexity.
Verification Method	Design Review

OCORA-498, B-Level - Safe and non-safe data exchange

The common standardised communication infrastructure supports safe data exchange for safety applications (SIL1 to SIL4) as well as non-safe data exchange for non-safe applications.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability. • To reduce overall integration complexity.
Verification Method	Design Review

3.1.2 Land-side communication

On one hand OCORA aims at simplifying the implementation of future land-side communication technologies and on the other hand aims at streamlining land-side communication infrastructure: to optimize equipment usage and to minimize equipment footprint (allocated space).

OCORA-576, B-Level - Isolate land-side communication

All land-side communication logic is strictly separated from other business logic.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To respect different life-cycles • Ensures replaceability & upgradeability
Verification Method	Design Review

OCORA-572, B-Level - Use FRMCS On-board System for train-land (land-train) communication

OCORA uses FRMCS technology for mission-critical, non-critical and voice communication.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To support trackside communication in areas where FRMCS is available
Verification Method	Design Review

OCORA-79, B-Level - Use GSM-R EDOR for train-land (land-train) data communication

OCORA supports using GSM-R EDOR for mission-critical, non-critical data communication

Status	✓ Approved
Req. Class	Requirement
Rationale	• To support trackside communication in areas where FRMCS is not yet available
Verification Method	Design Review

OCORA-611, B-Level - Use GSM-R for voice communication

OCORA supports using GSM-R for voice communication.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To support trackside communication in areas where FRMCS is not yet available
Verification Method	Design Review

OCORA-80, B-Level - Use Public Radio for train-land (land-train) data communication

OCORA supports using Public Radio for non-critical train-land data communication

Status	✓ Approved
Req. Class	Requirement
Rationale	• To support communication to the public network if not provided through FRMCS
Verification Method	Design Review

OCORA-81, B-Level - Ensure radio technology switching

OCORA allows switching between different radio technologies (GSM-R / FRMCS / Public) deployed on a vehicle.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To be able to operate in different expansion stages of the communication infrastructure (e.g switching between GSM-R and FRMCS for ETCS). • To be able to operate certain functionality over different communication infrastructure (e.g. monitoring over GSM-R, FRMC, Public).
Verification Method	Design Review

3.2 Platform Requirements

A generic safe or non-safe computing platform for onboard CCS applications, aims in particular to decouple applications from the underlying computing platform, considering their very distinct life cycles, and to achieve platform independence. Platform independence does neither address vehicle independence nor bearer independence, which are both important aspects of modularity and are covered in other chapters.

OCORA-619, B-Level - Aim for a standardised Computing Platform

Software building blocks run on a standardised computing platform.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability of software building blocks. • To reduce the number of hardware devices.
Verification Method	Design Review

OCORA-618, B-Level - Dedicated standardised Safe Computing Platform

Safe software building blocks run on a dedicated standardised safe Computing Platform.

Status	✓ Approved
Req. Class	Optional Requirement
Rationale	• To achieve "plug & play"-like exchangeability of software building blocks. • To reduce the number of hardware devices.
Verification Method	Design Review

OCORA-623, B-Level - Dedicated standardised Non-Safe Computing Platform

Non-safe software building blocks run on a dedicated standardised non-safe Computing Platform.

Status	✓ Approved
Req. Class	Optional Requirement
Rationale	• To achieve "plug & play"-like exchangeability of software building blocks. • To reduce the number of hardware devices.
Verification Method	Design Review

OCORA-170, B-Level - Standardised mixed criticality Computing Platform

Safe and non-safe software building blocks run side-by-side on the same standardised safe computing platform.

Status	✓ Approved
Req. Class	Optional Requirement
Rationale	• To achieve "plug & play"-like exchangeability of software building blocks. • To minimize the number of hardware devices.
Verification Method	Design Review

OCORA-487, B-Level - Platform Independence of Software Building Blocks

A Software Building Block, based on a generalised abstraction between the application logic and system interfaces, runs unchanged on different platform implementations.

Status	✓ Approved
Req. Class	Optional Requirement
Rationale	• Software building blocks are portable between platform instances of different vendors. • Building Block portability is a key enabler for the reduction of development costs.
Verification Method	Design Review

OCORA-570, B-Level - Provide mechanisms for remote (over-the-air) software updates

Software building blocks including their configurations can be safely and securely updated from remote e.g. without the need for physical presence of a maintenance operator.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To reduce maintenance cost • To be able to frequently apply security patches • To be able to deploy software/configuration/other artefact update quicker • To improve performance of operational systems e.g. faster deployment of bug fixes and similar (improved lifecycle)
Verification Method	Design Review

OCORA-622, B-Level - Provide mechanisms for local (on-board) software updates

Software building blocks including their configurations can be safely and securely updated locally (on-board) by a maintenance operator.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To be able to apply updates that are too big or complex to be downloaded over-the-air. • To have an alternative update path in case the over-the-air updates are not possible. • To allow software updates in case of a replacement of a defective device. • To allow maintenance when vehicle is in the work shop and not all systems of the vehicle are available.
Verification Method	Design Review

OCORA-620, B-Level - Provide mechanisms for remote (over-the-air) diagnostics & monitoring

OCORA provides mechanisms to collect diagnostics and monitoring information and forwards the data in batch or in near real-time to cerntralised diagnostics and monitoring services.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To allow for easier issue analysis • To simplify operational processes • To have information readily available in case of issues • To simplify fleet maintenance operations
Verification Method	Design Review

OCORA-621, B-Level - Provide mechanisms for local (on-board) diagnostics & monitoring

OCORA provides mechanisms to collect diagnostics and monitoring information and offers local (on-board) diagnostics and monitoring services.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To allow on-board issue analysis • To allow maintenance when vehicle is in the work shop and not all systems of the vehicle are available • To support commissioning and testing activities
Verification Method	Design Review

4 Quality and Performance Requirements

4.1 Interface Requirements

OCORA-119, B-Level - Standardised Communication Interface Specifications

All communication interfaces between building blocks and to external systems are specified and standardised on all OSI layers.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability of building blocks.
Verification Method	Design Review

OCORA-166, B-Level - Standardised Mechanical Interface Specifications

All external mechanical interfaces of physical building blocks are specified and standardised.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability of building blocks.
Verification Method	Design Review

OCORA-167, B-Level - Standardised Electrical Interface Specifications

All external electrical interfaces of physical building blocks are specified and standardised.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability of building blocks.
Verification Method	Design Review

4.2 RAMSS Requirements

OCORA-168, B-Level - Standardised and allocated RAMSS Specifications

The RAMSS requirements for each specific building block are specified and therefore standardised. This is valid for all building blocks.

Status	✓ Approved
Req. Class	Requirement
Rationale	• To achieve "plug & play"-like exchangeability of building blocks.
Verification Method	Design Review

4.3 Certification Requirements

OCORA-626, B-Level - Adhere to EN50155

The CCS on-board solution is designed according to EN 50155 (latest version including any amendments).

Status	✓ Approved
Req. Class	Requirement
Rationale	• Permits usage of electronic equipment used on rolling stock for railway applications
Verification Method	Process Review