

OCORA

Open CCS On-board Reference Architecture

GRAMSS Plan

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



Document ID: OCORA-TWS07-202

Version: 1.01

Date: 31.01.2025

Management Summary

This document is the Quality, RAM and Safety plan for OCORA as required for CENELEC V cycles in Phase 2 – System Definition. A first version of a [\[OCORA-TWS06-010\] - \(Cyber\) Security - Project Security Management Plan](#) was issued in OCORA R3 and is used as reference in the present the cyber-security activities in the context of the QRAMSS plan. As OCORA is not a legal organisation, neither a certification according to ISO 9001 is possible nor a ISA certificate. Based on that context, OCORA program follows a tailored EN 50126 quality management process (including RAM and Safety) where all steps are measured are presented in that document.

Revision history

Version	Change Description	Initial	Date of change
0.00	Initial draft	JB	22.07.2022
0.01	First draft for R4	JB	08.06.2023
0.02	Update draft for R4	JB	20.06.2023
1.00	Official version for R4	JB	28.06.2023
1.01	Editorial updates in the introduction chapter for R6	ML	31.01.2025

Table of contents

1	Introduction	13
1.1	Purpose of the document	13
1.2	Applicability of the document	13
1.3	Context of the document	13
1.4	Scope of the document	13
1.5	Responsibilities Related with the document	14
1.6	Update of the Document	14
2	OCORA description	14
2.1	OCORA Program	14
2.2	CCS OB System	15
2.3	Functional description	16
2.4	Architecture	16
2.5	Commercial off-the-shelf (COTS) and Re-used Components	17
2.6	Safety Principles	17
2.7	RAM Principles	17
2.8	Cyber-security Principles	17
3	Framework for QRAMSS Management	18
3.1	Context of OCORA	18
3.2	Project Management	19
3.3	Documentation management	19
3.3.1	Documentation identification	20
3.3.2	Documentation numbering	20
3.3.3	Documentation storage	21
3.3.4	Polarion documents generation	23
3.3.4.1	Polarion first page generation	23
3.3.4.2	Polarion document properties	23
3.3.4.3	Polarion document generation	24
3.3.5	Documentation maintenance	27
3.3.6	Documentation control sheet	28
3.4	Requirement management	28
3.5	Configuration Management	29
3.6	Change Management	29
3.7	Tool Management	29
3.8	Organization and Responsibilities	29
3.9	Limits of Responsibility	31
3.10	Operation and maintenance	31
3.11	Decommissioning and disposal	31
4	Safety Activities	32

4.1	Safety Management	34
4.1.1	Safety Planning	34
4.1.2	Hazard Log management	35
4.1.3	Model Based Safety Analysis	35
4.2	Overall OCORA Lifecycle	36
4.3	Phase 1 "Concept"	36
4.3.1	Objective	36
4.3.2	Activities	36
4.3.2.1	OCORA initiative	36
4.3.2.2	Building Blocks suppliers	36
4.3.2.3	Integrators	36
4.3.2.4	Railway Undertakings	37
4.4	Phase 2 "System Definition and Operational Context"	37
4.4.1	Objective	37
4.4.2	Activities	37
4.4.2.1	OCORA initiative	37
4.4.2.1.1	GRAMSS Plan	37
4.4.2.1.2	MBSA - Operational Safety Analysis	37
4.4.2.1.3	System Definition	38
4.4.2.2	Building Blocks suppliers	38
4.4.2.3	Integrators	38
4.4.2.4	Railway Undertakings	38
4.5	Phase 3 "Risk Analysis and Evaluation"	38
4.5.1	Objective	38
4.5.2	Activities	39
4.5.2.1	OCORA initiative	39
4.5.2.1.1	Risk Analysis	39
4.5.2.1.2	Hazard Log	40
4.6	Phase 4 "Specification of System Requirements"	41
4.6.1	Objective	41
4.6.2	Activities	41
4.6.2.1	OCORA initiative	41
4.6.2.1.1	MBSA - System Hazard Analysis	41
4.6.2.1.2	OCORA Safety requirements	41
4.6.2.1.3	Independent Safety Assessment	42
4.6.2.2	Building Blocks suppliers	42
4.6.2.3	Integrators	42
4.6.2.4	Railway Undertakings	42
4.7	Phase 5 "Architecture and apportionment of system requirements"	42
4.7.1	Objective	42

4.7.2	Activities	43
4.7.2.1	OCORA initiative	43
4.7.2.1.1	Interface Hazard Analysis	43
4.7.2.1.2	Fault tree analysis	43
4.7.2.1.3	OCORA Safety requirements	43
4.7.2.1.4	Design Safety Case	45
4.7.2.1.5	Independent Safety Assessment	45
4.7.2.2	Building Blocks suppliers	46
4.7.2.3	Integrators	46
4.7.2.4	Railway Undertakings	46
4.8	Phase 6 "Design and implementation"	46
4.8.1	Objective	46
4.8.2	Activities and responsibilities	46
4.8.2.1	OCORA initiative	46
4.8.2.2	Building Blocks suppliers	47
4.8.2.3	Integrators	47
4.8.2.4	Railway Undertakings	47
4.9	Phase 7 "Manufacture"	47
4.9.1	Objective	47
4.9.2	Activities	47
4.9.2.1	OCORA initiative	47
4.9.2.2	Building Blocks suppliers	47
4.9.2.3	Integrators	47
4.9.2.4	Railway Undertakings	47
4.10	Phase 8 "Integration"	48
4.10.1	Objective	48
4.10.2	Activities	48
4.10.2.1	OCORA initiative	48
4.10.2.2	Building Blocks suppliers	48
4.10.2.3	Integrators	48
4.10.2.4	Railway Undertakings	48
4.11	Phase 9 "System Validation"	48
4.11.1	Objective	48
4.11.2	Activities	49
4.11.2.1	OCORA initiative	49
4.11.2.2	Building Blocks suppliers	49
4.11.2.3	Integrators	49
4.11.2.4	Railway Undertakings	49
4.12	Phase 10 "System acceptance"	49
4.12.1	Objective	49

4.12.2	Activities	49
4.12.2.1	OCORA initiative	49
4.12.2.2	Building Blocks suppliers	49
4.12.2.3	Integrators	49
4.12.2.4	Railway Undertakings	50
4.13	Phase 11 "Operation, maintenance and performance monitoring"	50
4.13.1	Objective	50
4.13.2	Activities	50
4.13.2.1	OCORA initiative	50
4.13.2.2	Building Blocks suppliers	50
4.13.2.3	Integrators	50
4.13.2.4	Railway Undertakings	50
4.14	Phase 12 "Decommissioning"	51
4.14.1	Objective	51
4.14.2	Activities	51
4.14.2.1	OCORA initiative	51
4.14.2.2	Building Blocks suppliers	51
4.14.2.3	Integrators	51
4.14.2.4	Railway Undertakings	51
5	RAM Activities	52
5.1	Objectives	52
5.1.1	RAM	52
5.1.2	Life Cycle Cost (LCC)	52
5.2	Approach	52
5.2.1	Introduction	52
5.3	Phase 1 "Concept"	53
5.3.1	Objective	53
5.3.2	Activities	53
5.3.3	Phase 2 "System Definition and Operational Context"	54
5.3.4	Objective	54
5.3.5	Activities	54
5.4	Phase 3 "Risk Analysis and Evaluation"	54
5.4.1	Objective	54
5.4.2	Activities	54
5.5	Phase 4 "Specification of System Requirements"	54
5.5.1	Objective	54
5.5.2	Activities	55
5.6	Phase 5 "Architecture and apportionment of system requirements"	55
5.6.1	Objective	55
5.6.2	Activities	55

6 Cyber-security Activities	56
7 Synchronisation activities	57
8 Decisions and issues	58
8.1 Decisions	58
8.2 Issues	58
9 Annex - QRAMSS deliverables	59

Table of figures

Figure 1 CENELEC Arrangement for independence

Figure 2 OCORA requirements in the V cycle

Figure 3 OCORA requirements in the V cycle

with the following dataFigure 4 Polarion Wiki contentwith the following datawith the following datawith the following data

Figure 5 Result of a successful addition of wiki content

Figure 6 Configure Doc Properties in Polarion

Figure 7 PDF extract for Polarion artifacts

Figure 8 Extract to PDF pop-up

Figure 9 "Configure" PDF pop-up

Figure 10 CENELEC Arrangement for independence

Figure 11 OCORA Requirements Structure from Project Input Sources

Figure 12 OCORA requirements in the V cycle

Figure 13 OCORA Releases into the V-cycle

Figure 14 MBSE structure in EN 50126 V cycle

Figure 15 SRAC emission strategy

Figure 16 Refinement of safety requirements

Figure 17: Phases from EN 50126-1 covered in the RAM Plan According to the EN 50126-1:

Table of tables

Table 1 Responsibilities

Table 2 Frequency of Occurrence Classification

Table 3 Hazard Severity Level

Table 4 Risk Evaluation and Acceptance

Table 5 Qualitative Risk Categories

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 reference 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](#)
- [\[OCORA-BWS02-020\] - Program Slide Deck](#)
- [\[OCORA-BWS02-030\] - Technical Slide Deck](#)
- [\[OCORA-BWS02-040\] - Program Posters](#)
- [\[OCORA-BWS02-050\] - Technical Posters](#)
- [\[OCORA-BWS02-060\] - Confidentiality Clause](#)
- [\[OCORA-BWS03-010\] - Introduction to OCORA](#)
- [\[OCORA-BWS03-020\] - Guiding Principles](#)
- [\[OCORA-BWS04-010\] - Problem Statements](#)
- [\[OCORA-BWS05-010\] - Road Map](#)
- [\[OCORA-BWS05-020\] - Minimal Viable Product](#)
- [\[OCORA-BWS06-010\] - Economic Model - Guiding Principles, Main Assumptions, General Assessment Criteria](#)
- [\[OCORA-BWS06-020\] – Economic Model](#)
- [\[OCORA-BWS06-030\] - Economic Model - Software Requirements Specification](#)
- [\[OCORA-BWS06-040\] - Economic Model - User Manual](#)
- [\[OCORA-BWS06-050\] - Economic Model - CCS System Life Cycle Costing Scenario Studies](#)
- [\[OCORA-BWS06-060\] - Economic Model - CCS impact on Vehicle System Life Cycle Costing Scenario Studies](#)
- [\[OCORA-BWS07-010\] - Alliances](#)
- [\[OCORA-BWS08-010\] - Methodology](#)
- [\[OCORA-BWS08-020\] - Tooling](#)
- [\[OCORA-BWS09-010\] - Acceptance of Global Standards](#)
- [\[OCORA-BWS09-020\] - Acceptance of Global Standards - Focus on Safety in CCS](#)
- [\[OCORA-BWS09-030\] - Acceptance of Global Standards - Cross-Acceptance Guideline](#)
- [\[OCORA-TWS01-010\] – Design Requirements](#)
- [\[OCORA-TWS01-011\] – System Requirements](#)
- [\[OCORA-TWS01-020\] – System Capabilities](#)
- [\[OCORA-TWS01-030\] – System Architecture](#)
- [\[OCORA-TWS01-035\] – CCS-On-Board Architecture](#)
- [\[OCORA-TWS01-040\] – Capella Modelling](#)
- [\[OCORA-TWS01-041\] - MBSE-Modelling-Guideline](#)
- [\[OCORA-TWS01-050\] – Capella Model Extract](#)
- [\[OCORA-TWS01-100\] – Localisation On-Board \(LOC-OB\) – Introduction](#)
- [\[OCORA-TWS01-101\] – Localisation On-Board \(LOC-OB\) – Requirements](#)
- [\[OCORA-TWS01-102\] – Localisation On-Board \(LOC-OB\) – Standard Communication Interface Specification](#)
- [\[OCORA-TWS02-010\] – CCS Communication Network \(CCN\) – Evaluation](#)
- [\[OCORA-TWS02-020\] – CCS Communication Network \(CCN\) – Proof of Concept](#)
- [\[OCORA-TWS03-010\] – Generic Safe Computing Platform for Railway Applications – Whitepaper](#)

- [OCORA-TWS03-020] – Generic Safe Computing Platform for Railway Applications – Requirements
- [OCORA-TWS03-030] - An Approach for a Platform Independent API
- [OCORA-TWS04-010] - Functional Vehicle Adapter – Introduction
- [OCORA-TWS04-013] – Functional Vehicle Adapter – Design Guideline
- [OCORA-TWS04-011] – Functional Vehicle Adapter – Requirements
- [OCORA-TWS04-020] - Functional Vehicle Adapter - Standard Communication Interface Specification
- [OCORA-TWS04-030] - Functional Vehicle Adapter – Design Guideline
- [OCORA-TWS04-040] – Gap Analysis (SUBSET-119)
- [OCORA-TWS05-010] – Requirements – Management Guideline
- [OCORA-TWS05-020] – Stakeholder Requirements
- [OCORA-TWS05-021] – Program Requirements
- [OCORA-TWS05-022] – Design Requirements
- [OCORA-TWS06-010] - (Cyber) Security - Project Security Management Plan
- [OCORA-TWS06-011] – (Cyber-) Security – Requirements
- [OCORA-TWS06-020] - (Cyber) Security - Guideline
- [OCORA-TWS07-010] - Modular Safety – Strategy
- [OCORA-TWS07-011] – Modular Safety – Requirements
- [OCORA-TWS07-020] - RAMS Evolution management
- [OCORA-TWS07-030] - RAMS SRAC-AC Management
- [OCORA-TWS07-040] - RAMS Optimized Approval Process
- [OCORA-TWS07-050] – RAMS – RAM Strategy
- [OCORA-TWS07-060] - Configuration Management Concept
- [OCORA-TWS07-100] – CENELEC Phase 1 – System Concept
- [OCORA-TWS09-010] - Testing - Strategy
- [OCORA-TWS09-011] – Testing – Requirements
- [OCORA-TWS09-020] – Testing – Benchmarking Report Modular Testing
- [OCORA-TWS09-040] - Common Control Network Testing Strategy
- [OCORA-TWS09-050] - (Cyber) Security Testing Strategy
- [EN 50126-1:2017-10] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
- [EN 50126-2:2017-10] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
- [EN 50128:2011-06] – Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems
- [EN 50129:2018-11] – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
- [EN 50155: 2017] – Railway applications – Rolling stock – Electronic equipment
- [EN 50159:2010-09] – Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
- [EN 50657:2017-08] - Railways Applications - Rolling stock applications - Software on Board Rolling Stock
- prEN 50701 - Railway applications - Cybersecurity
- TSI CCS: 02016R0919
- [SUBSET-091]
- [ISO/IEC 7498-1:1994] - Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model - Part 1
- [ERA ERTMS 015560] – ETCS Driver Machine Interface
- [EUG 97E2675B] - ERTMS User Group Document 97E2675B

- [EN 15380-4] - Railway applications - Classification system for railway vehicles - Function groups
- [ISBN 978-1-78548-169-7] – Model-based System and Architecture Engineering with the Arcadia Method – Jean Luc Voirin – ISTE Press - 01/03/2018
- [EUG 21E109] - Vehicle Locator Concept Architecture, LWG, version 1.0, 2021-07-15
- [ISO/IEC 15288:2015] Systems and software engineering — System life cycle processes, 2015
- [ERA 1209-063] Clarification note on safe integration
- [Directive 2018/545]

1 Introduction

1.1 Purpose of the document

The purpose of this document is to present the roadmap of Quality, RAM, Safety and cyber-security activities performed in the OCORA program.

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 [\[OCORA-BWS01-040\] – Feedback Form](#).

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

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

1.2 Applicability of the document

The document is informative. 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 an OCORA Release, together with the documents listed in the release notes [\[OCORA-BWS01-010\] – Release Notes](#). Before reading this document, it is recommended to read the Release Notes [\[OCORA-BWS01-010\] – Release Notes](#). If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [\[OCORA-BWS03-010\] - Introduction to OCORA](#), the Guiding Principles [\[OCORA-BWS03-020\] - Guiding Principles](#), the Problem Statements [\[OCORA-BWS04-010\] - Problem Statements](#), and the Road Map [\[OCORA-BWS05-010\] - Road Map](#). The reader should also be aware of the Glossary [\[OCORA-BWS01-020\] – Glossary](#) and the Question and Answers [\[OCORA-BWS01-030\] – Question and Answers](#).

1.4 Scope of the document

This document intends to present the lifecycle activities of the OCORA program regarding Quality/RAM/Safety and cyber-security management. As presented in [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#), the OCORA program covers the CENELEC phases 1 to 5. The phases 6 to 12 will be realised by the industry suppliers developing the OCORA compliant building blocks. Therefore, these phases are not part of the present QRAMSS plan.

This document covers the whole OCORA program scope; the CCS OB system, and all parallel “V cycles” deployed for the key OCORA elements which are defined in [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#) and summarised in section 2.2. This documents lists all QRAMSS deliverables and indicate for each of them if it is a common document for all sub-systems or realised within each sub V cycle.

1.5 Responsibilities Related with the document

This document is:

- written by RAMS managers of the TWS07
- verified by other RAMS Managers and the TWS07 leader
- approved by the OCORA Core team

1.6 Update of the Document

The QRAMSS Plan will be updated and reviewed in case of significant changes occurred during the OCORA program lifetime.

Any new version of the QRAMSS Plan is produced, verified and approved in compliance with responsibilities defined in [OCORA-7930 - Responsibilities Related with the document](#) and following [OCORA-7939 - Framework for QRAMSS Management](#). The main reasons causing the updates have to be reported in the Revision history (e.g. organization changes, scope, developments change and/or modified techniques to be applied, ..).

2 OCORA description

2.1 OCORA Program

The OCORA program is defined in documents:

- [\[OCORA-BWS02-030\] - Technical Slide Deck](#),
- [\[OCORA-BWS03-010\] - Introduction to OCORA](#),
- [\[OCORA-TWS05-020\] – Stakeholder Requirements](#).

The followings sentences are extracted from [\[OCORA-BWS03-010\] - Introduction to OCORA](#):

OCORA is first and foremost a platform for cooperation to the benefit of the European Railway sector. [\[OCORA-BWS03-020\] - Guiding Principles](#) rules and regulations agreed between OCORA members, are expressed in the OCORA Memorandum of Understanding (MoU) and the OCORA Code of Conduct (CoC).

Members collaborate on the development of an open reference architecture for on-board command-control and signalling systems that supports the mutually agreed OCORA objectives (Chapter 6). Collaboration takes place in working groups. Each working group is responsible for specific tasks, topics or issues. Working group(s) and participating experts are appointed by the OCORA management team.

OCORA is not a legal entity and cannot exert owner rights. In case collaboration projects would lead to financial commitments for the members, these commitments will have to be formally agreed prior to execution.

The founding members of OCORA are:

- Deutsche Bahn AG
- Schweizerische Bundesbahnen SBB
- NS Groep N.V.
- SNCF for itself and in the name of SNCF Voyageurs and SNCF Réseau
- ÖBB-Produktion GmbH

OCORA is open to any railway undertaking or train keeper willing to accept the MoU and CoC. Ideally, all members are having delegates that actively support one or several working groups.

OCORA-330 - Open Collaboration

The OCORA initiative shall be an open collaborative technical platform open to any railway company, for instance railway undertakings, fleet keepers or owners. It is based on sharing subject matter expertise and making publicly available its deliverables for the benefit of the whole railway sector. All members bring into the collaboration experiences, practice among CCS On-board and use OCORA Requirements for CCS purchase to establish a de facto standard.

OCORA-53 - Reduce Total Cost of Ownership

The OCORA Reference architecture shall reduce the amount of capital and operational expenditure for a CCS On-Board, taking into account the full life cycle.

OCORA-54 - Shorter Time2Market

The OCORA initiative shall reduce the amount of time to introduce CCS On-board in general, as well as, new or adapted CCS functionalities into a new or an existing vehicle, taking into account the following scope:

- Unifying User Requirements
- TSI improvement
- Specification
- Design
- Development
- Integration
- Testing
- Verification
- Validation
- Certification
- Rollout
- Service / Operation

OCORA-61 - Support different vehicle types

The OCORA initiative shall consider Passenger Trains, Cargo Trains as well as Construction Trains (on track machines) when defining the OCORA architecture.

OCORA-1203 - Reduction of one-off product efforts

The OCORA initiative shall minimize the effort spent for requirement engineering, specification and development of CCS On-board as a product.

OCORA-326 - Reduction of one-off integration efforts

The OCORA initiative shall minimize engineering and certification effort needed for adjusting CCS On-board to specific vehicle types / fleets.

OCORA-55 - Increase performance

The OCORA initiative shall increase reliability, availability, maintainability and security of the CCS on-board solution whilst maintaining the current level of safety. Targets for each performance category shall be elaborated and set after the development of the OCORA RAM Model.

2.2 CCS OB System

The SuC of OCORA is the CCS-OB system with the scope defined in the [TSI CCS: 02016R0919](#). The latter is defined in [[OCORA-BWS02-030](#)] - Technical Slide Deck, and [[OCORA-TWS01-030](#)] – System Architecture. and summarized in the [[OCORA-TWS07-100](#)] – CENELEC Phase 1 – System Concept.

OCORA-500 - Standardised CCS on-board system for different vehicle types

The OCORA reference architecture shall minimize the required integration effort for introducing CCS on-board into different vehicle types, ensuring plug-&-play" like deployment and efficient development, certification, installation and maintenance.

The simplicity and effort related to the "plug-&-play" vision is expected to develop over time depending on technical readiness level.

OCORA-501 - CCS on-board consists of separately sourceable building blocks

The OCORA initiative shall decompose the CCS on-board system into an optimal and reasonable number of standardized building blocks

OCORA-499 - Standardised Interface to the Vehicle

Communication between the CCS on-board and the vehicle shall be realised through a vehicle independent, standardised interface.

2.3 Functional description

The functional description is defined by the System Capabilities WP11 of TWS01 [OCORA-TWS01-020] – System Capabilities. At this level of the OCORA program, the complete functional definition of the SuC has not been provided (refer to OCORA-10238 - No overall functional breakdown available).

2.4 Architecture

The OCORA program defines the overall architecture of the future CCS OB systems which is based on standardised and interoperable building blocks (hardware and software building blocks). The decomposition is presented below:

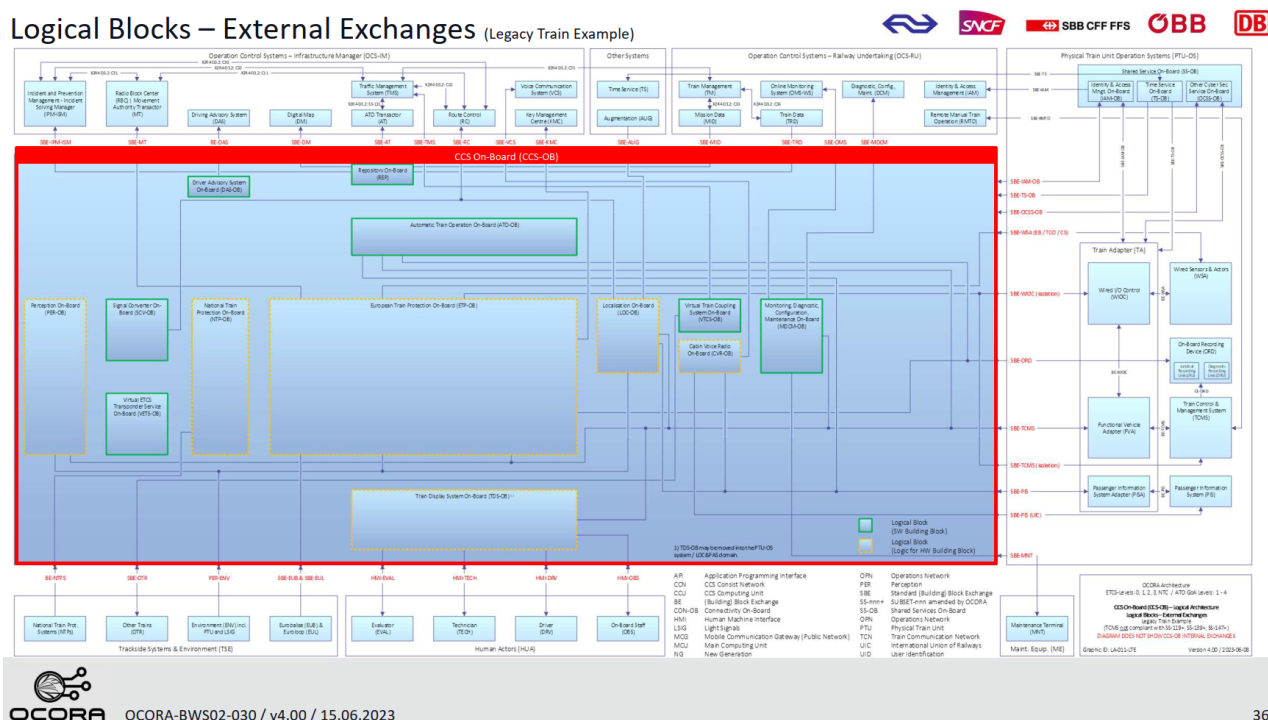


Figure 1 CENELEC Arrangement for independence

Therefore, the OCORA CCS OB system can be assembled with the following hardware building blocks:

- European Train Protection on-board (ETP-OB),
- Localisation on-board (LOC-OB),
- Cabin Voice Radio on-board (CVR-OB),
- National Train Protection on-board (NTP-OB),
- Train Display System on-board (TDS-OB),
- UID Reader on-board (UIDR-OB)
- Perception System on-board (PER-OB)

OCORA CCS OB system also integrated software building blocks (i.e. application hosted on 1 or several computing platform defined in [OCORA-TWS03-010] – Generic Safe Computing Platform for Railway Applications – Whitepaper). These software building blocks covers both exiting functions defined in TSI CCS: 02016R0919 and new ones still under

definition:

- Digital map Repository on-board (DREP-OB),
- Driver Advisory System on-board (DAS-OB),
- Automatic Train Operation on-board GoA1-4 (ATO-OB),
- Virtual Train Coupling System on-board (VTCS-OB),
- Monitoring, Diagnostic, Configuration, Maintenance on-board (MDCDM-OB),
- Remote Manual Train Operation on-board (RMTO-OB),
- Signal Converter on-board (SCV-OB),
- Virtual ETCS Transponder Service on-board (VETS-OB).

The functional allocation for each building block will be performed in a future release of OCORA and will be analysed by the RAMS team during phase 3 (risk identifications linked to the new functionalities) and phase 4 (analysis of the functional breakdown).

It must be noticed that the OCORA program defines the overall architecture of the CCS OB with its decomposition in building blocks, their addressed functions and all RAMS requirements (including TFFR).

The internal design of each building block is on the discretion of each vendor as long as the OCORA set of requirements (i.e. call for tender requirements) are respected. This is defined in [OCORA-8637 - Building Blocks suppliers](#).

2.5 Commercial off-the-shelf (COTS) and Re-used Components

The OCORA initiative is an R&I program which aim to propose at the end sets of requirements for future standardized and interoperable building block. In addition, as the project will end in Phase 5 of EN 50126 V-cycle, no design activities will be performed within the OCORA program.

Therefore, there will be no COTS or re-used components in the scope of OCORA. This section is then not applicable.

2.6 Safety Principles

As presented in the [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#), the OCORA program must be designed in conformity with [TSI CCS: 02016R0919](#) and therefore according to [\[SUBSET-091\]](#) for all safety aspects of existing functions. This means that all hazards and the on-board THR must be integrated covered by the OCORA design. In case some of the hazards presented in SUBSET-091 are not applicable to OCORA, they must be justified in the OCORA Hazard Log (to be created in a future release of OCORA).

The new version of TSI CCS: 2023 including updated and new safety subsets will also be considered in the next OCORA release especially regarding the new functions not covered yet by the latest applicable version (e.g. ATO OB). All new hazards will therefore be considered into OCORA design and covered in a to be created future release of OCORA).

2.7 RAM Principles

Today, no RAM subset exists nor harmonised RAM target at European level. Therefore, the OCORA RAM team will consider as RAM principles the existing RAM data coming from the OCORA members after they have been harmonised and commonly agreed.

2.8 Cyber-security Principles

Cyber-security principles are defined in the [\[OCORA-TWS06-010\] - \(Cyber\) Security - Project Security Management Plan](#).

3 Framework for QRAMSS Management

This section presents the overall strategy involving Quality, RAM, Safety, Cyber-security and the organization in terms of responsibilities adopted by OCORA to ensure that the documentation deliveries for the CCS OB system and its building blocks meets its functional, operational and QRAMSS expectations.

The QRAMSS strategy and the organization described in this plan must be done in accordance with standards [EN 50126-1:2017-10] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, [EN 50129:2018-11] – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, [EN 50128:2011-06] – Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems, [EN 50657:2017-08] - Railways Applications - Rolling stock applications - Software on Board Rolling Stock, [EN 50129:2018-11] – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling and prEN 50701 - Railway applications - Cybersecurity.

The implementation of a strong and adapted quality management is a prerequisite to develop a RAMSS critical project in a healthy way. It aims at decreasing significantly the occurrence of systematic failures. However, its complete application is not foreseen for every project and tailoring is allowed whenever needed if relevant justifications are provided. This is explicitly presented by EN 50126-1:

The process defined by this European Standard assumes that railway duty holders and railway suppliers have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within EN ISO 9001.

[...]

The quality management system should conform to EN ISO 9001 rules or equivalent rules and be appropriate for the system under consideration;

NOTE Conformity to these requirements is sufficient for the quality management of the RAM requirements and is a necessary basis for the safety management which is needed to fulfil the safety requirements;

[...]

The application of this standard may be tailored allowing requirements of Clause 7 to be scaled to the specific requirements for the system under consideration. This tailoring should consider the following aspects:

- *constraints given by the railway duty holder;*
- *complexity of the system under consideration;*
- *the application domain (i.e. signalling, rolling stock, fixed installations);*
- *the system development process used;*
- *type of development (e.g. generic product, specific application, modification of existing system).*

The process may be simplified by reusing existing applicable material.

3.1 Context of OCORA

OCORA is a European initiative composed of five RU companies without a legal entity. That means the OCORA program cannot rely a quality management accredited to EN ISO 9001. In addition to that, OCORA program is intended to provide documentation to be used by railway manufacturers during the call for tenders (i.e. usually called Requirements Book) to create the future CCS OB system and its building blocks. The OCORA initiative takes inspiration from [TSI CCS: 02016R0919](#) and its SUBSETS to realise its documentation. The latter does not cover the full V cycle from EN50126-1 but focuses on phase 1 to 5 (including phase 0 from TS 50701) as presented below.

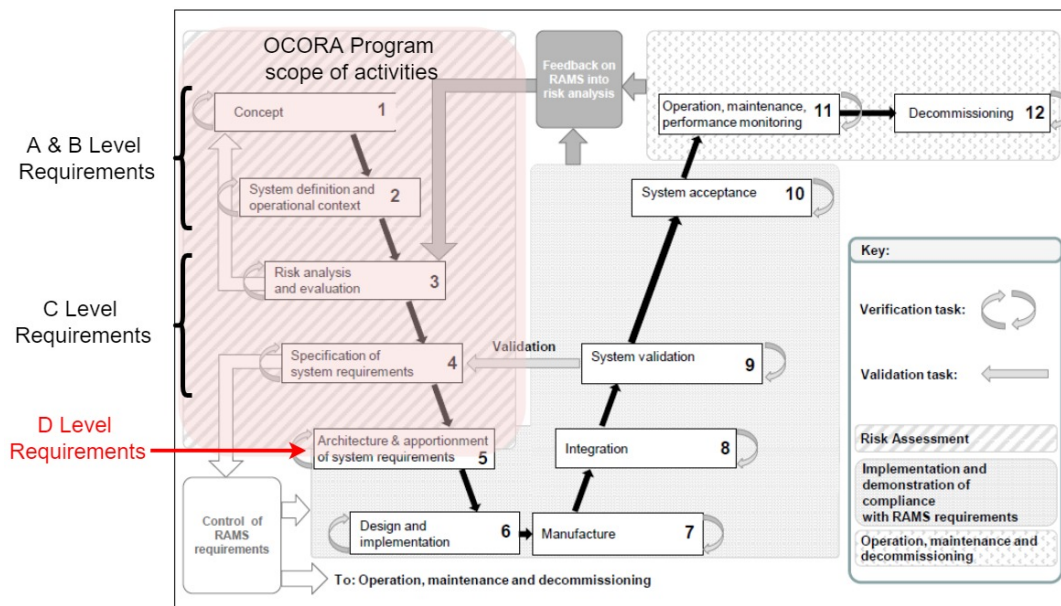


Figure 2 OCORA requirements in the V cycle

From Figure 2, this means that:

- the "Risk Assessment" phase are covered by the OCORA program,
- the "Implementation and demonstration of compliance with RAMS requirements" phase will be held by the manufacturers and the integrators,
- the "Operation, maintenance and decommissioning" phase will be handled by RU's.

The OCORA program is thus focusing on documentation activities without any implementation or realisation (e.g. hardware or software elements). Based on that, the quality management to be deployed can be tailored from a usual one defined into RU's or manufacturers. The latter focuses on the following aspects:

- OCORA-8020 - [Documentation management](#) ,
- OCORA-8021 - [Requirement management](#) ,
- OCORA-7951 - [Synchronisation activities](#) .

3.2 Project Management

The project management rules for the OCORA program is introduced in [\[OCORA-BWS07-010\] - Alliances](#) and developed in [\[OCORA-BWS08-010\] - Methodology](#). This activity is handled by the OCORA Core team (see [OCORA-7945 - Organization and Responsibilities](#)).

3.3 Documentation management

Documentation management (e.g. single identification, single versioning strategy) is a key mandatory point to comply with EN 50126 expectation to decrease the occurrence of systematic failures. This is presented in section 6.6 of EN 50126-1:

6.6 General requirements on RAMS documentation

A RAM Plan and a Safety Plan shall be established identifying the documents recording information relevant to RAMS throughout the life cycle of the system under consideration.

A process for the maintenance of RAMS documentation shall be defined or referenced in the RAM Plan and Safety Plan. For each document, traceability shall be provided in terms of a unique reference number (including version) including a defined and documented relationship with other documents.

Each RAMS document and deliverable shall be placed under configuration control from the time of its first release. Any changes to documents under configuration control shall be recorded.

The subsections hereafter aims at presenting the OCORA initiative strategy for dealing with documentation management.

3.3.1 Documentation identification

Each deliverable document from the OCORA program shall be identified through a unique reference as required by EN 50126-1 section 6.6:

For each document, traceability shall be provided in terms of a unique reference number (including version) including a defined and documented relationship with other documents.

A documentation naming strategy is defined for the different types of artifacts possible:

- OCORA-xWSnn-nnn_ExcelFileName for all Excel type documents,
- OCORA-xWSnn-nnn_PresentationTitle for all PowerPoint type documents ,
- OCORA-xWSnn-nnn_WordDocumentTitle-Subtitle for all Word type documents,
- OCORA-xWSnn-nnn_WordPosterTitle for all Word type poster

The customisation consists in fulfilling the different items:

- **x** refers to the type of OCORA workstream:
 - **B** for Business workstream,
 - **T** for Technical workstream,
- **WSnn** refers to the number of the OCORA workstream considered between 00 and 99
- **nnn** refers to the number of the document between 001 and 999. This number is independent from the workstream number. In mean that each workstream can pick numbers between 001 and 999.

The harmonisation and coherency of the whole OCORA documentation is ensured by a synchronisation file called *OCORA-BWS00-010_Documentation_Plan*. Each workstream leader is in charge of managing his own documentation and fulfil the file with all references. This documentation plan is used as basis to control the amount of artifacts produced by each OCORA release. Its update is ensured by the OCORA Core team.

The *OCORA-BWS00-010_Documentation_Plan* shall be managed by the OCORA Core team.

Each WS leader shall provide to the core team data concerning the documentation produced in their related WS.

A quality check shall be done before each OCORA release delivery and/or before ending each CENELEC phase (i.e. 2 to 5) that all OCORA artifacts' names are in line with the quality (i.e. template naming) rules and the documentation plan.

3.3.2 Documentation numbering

The OCORA intends to define an harmonised strategy for documentation numbering among the different workstreams.

Each author shall use the "x.yz" strategy for his/her documentation numbering:

- **x**: starts at 0 and is incremented at each new OCORA release if and only if important changes are added to the document,
- **y**: minor updates (e.g. late comments taken in account, adjustments regarding other OCORA deliverables) are handled under the latest "x" used with an incrementation of a "y" digit (e.g. from 1.12 -> 1.20) where "yz" can then be again incremented from 1.20 to 1.yz,
- **z**: draft updates. this digit is used to increment each new draft available in case of major or minor update of the document. "yx" digits can be incremented from 00 to 99.

Here are some examples of possible incrementation of numbers:

- Change of major version:
 - OCORA R3 official version **1.20**

- OCORA R4 starting version: **2.00**
 - Update of the document with different drafts: **2.01** to **2.11**
 - OCORA R4 last draft: **2.11**
 - OCORA R3 official version: **2.11**
-
- Change of minor version:
 - CORA R3 official version **3.24**
 - OCORA R4 starting version: **3.30**
 - Update of the document with different drafts: **3.31** to **3.38**
 - OCORA R4 last draft: **3.38**
 - OCORA R3 official version: **3.39** (CORE team required few typo updates).

3.3.3 Documentation storage

The OCORA Program intends to provide public documentation for future call for tenders with industry partners. As OCORA is not a legal entity, the documentaion storage must be done on a neutral place, meaning not owned by any company involved in OCORA (i.e. DB, NS, ÖBB, SBB or SNCF). The core team decided to choose the open platform GitHub to reach that.

Unfortunately, GitHub is not made does not allow a collaborative work on the artefacts in a simultaneous way compared to tools like SharePoint. On the other hand, SharePoint is not a recognized tool to perform documentation management as required by EN 50216-1.

For that reason, the CORE team has decided to us both tools with clear scopes as presented on Figure 3.

A third tool, covering requirements and document management is deployed within OCORA; Polarion. Its use within OCORA is presented in documents [\[OCORA-BWS08-010\] - Methodology](#) and [\[OCORA-TWS05-010\] – Requirements – Management Guideline](#) and in section [OCORA-10192 - Polarion documents generation](#).

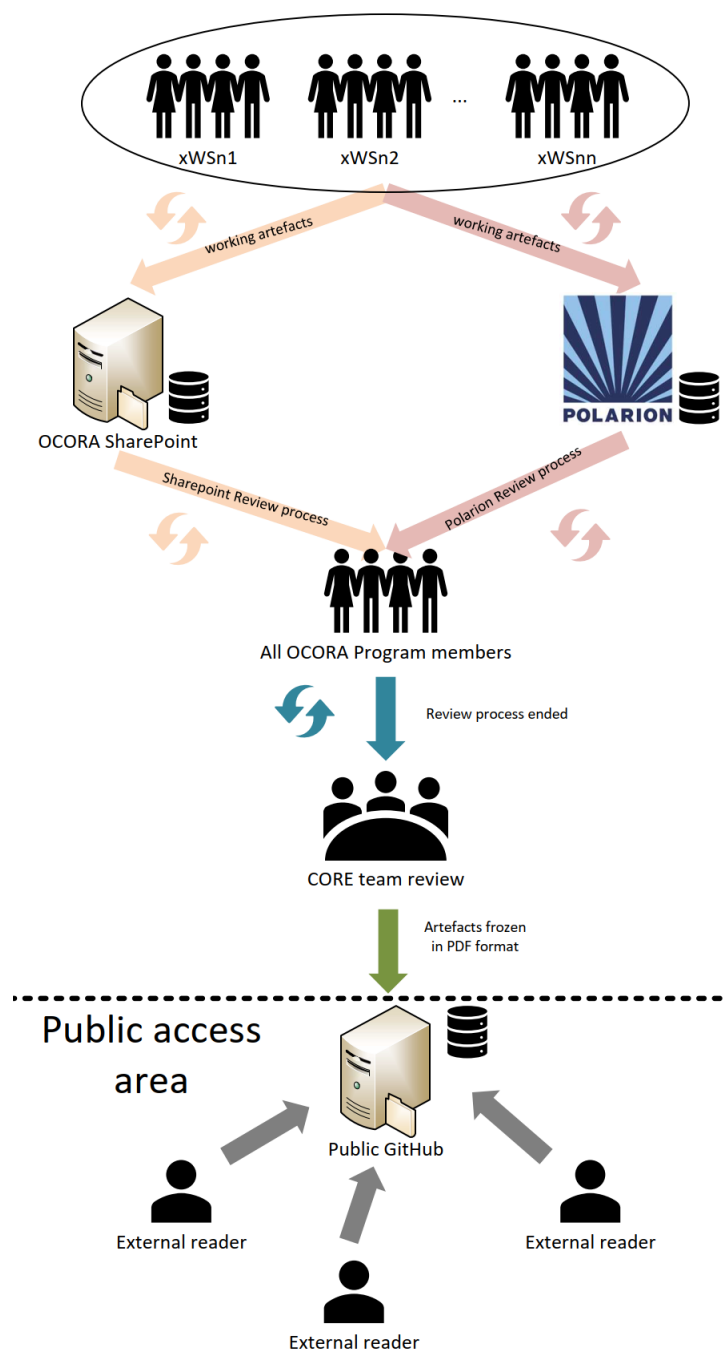


Figure 3 OCORA requirements in the V cycle

Each business and technical workstream is invited to use a SharePoint belonging to one of the OCORA member to realise their OCORA artefacts in a collaborative way. This activity is limited to the creation of the draft versions of the documents, including internal review (i.e. among the same workstream).

To help at having these activities done in the most efficient way, each team is invited to use track changes and interactive comments whenever possible.

The quality management does not provide any mandatory requirements for this working phase of the artifacts. It is the responsibility of each workstream leader to define the rules to be applied for each document to finally be able to provide at the date excepted by the core team a complete and agreed (i.e. no more internal comments opened) draft version for other workstream reviews.

From that moment, each workstream leader is invited to push all mature draft documents into a single and common review folder located on private GitHub. The path is always following the same strategy:

OCORA\02_Alliance & Communication\03_Communication\03_OCORA Releases\nn_Release-xx\Review_Versions

In parallel, each workstream leader communicates to the the other workstream who are the mandatory reviewers of the

documents. In case of consistent artefacts, the leader is invited to identify sections or parts of the documents where each mandatory reader must have a critical eye. This helps each reviewer to focus on relevant points where his opinion is the most relevant and avoid wasting unproductive hours of documentation reading before each delivery.

3.3.4 Polarion documents generation

The OCORA initiative requires that all documents containing requirements shall be created and managed in Polarion.

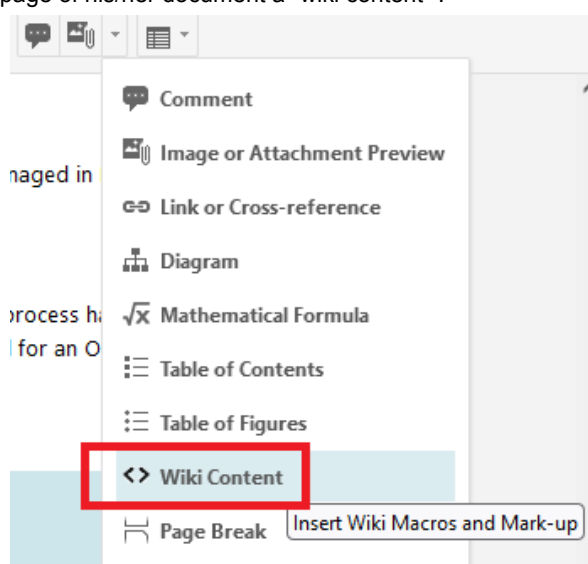
OCORA-461 - Use Polarion for requirements management

The OCORA initiative shall use Polarion for requirement engineering and management

To get an harmonised set of documents coming from SharePoint and Polarion, a dedicated small process has been defined to help the author of a Polarion document to set-up the tool for a succesfull PDF file generation, used for an OCORA official delivery.

3.3.4.1 Polarion first page generation

Each author shall add in the first page of his/her document a "wiki content" :



with the following dataFigure 4 Polarion Wiki contentwith the following datawith the following datawith the following data

and fill it with the following content:

```
#includeMacros("macros.titlePageOCORA")
#printTitlePageInDocument()
```

Finally, the front page is no more visible, only the "wiki" logo.

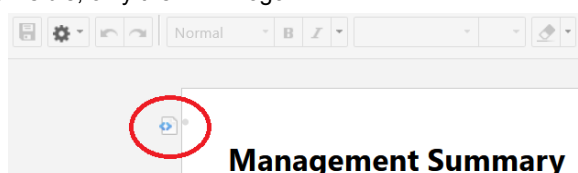


Figure 5 Result of a successful addition of wiki content

3.3.4.2 Polarion document properties

Each author shall fill the document properties of his/her Polarion document. This aims at filling the information of the documents and its first page.

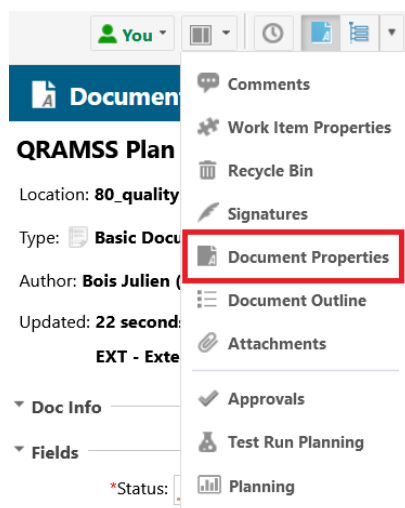


Figure 6 Configure Doc Properties in Polarion

All following fields shall be filled:

- Status: to be filled according to the Polarion process for reviewing artifacts (refer to [\[OCORA-BWS08-010\] - Methodology](#)),
- Owner: to be filled with the author's name,
- Version: to be filled according to [OCORA-10198 - Documentation numbering](#),
- Language: to be filled with the official language of OCORA: English,
- Classification: by default, documents are set as "internal",
- Release Date: to be filled with the date when the document is generated
- Document ID: to be filled according to

3.3.4.3 Polarion document generation

Each other shall provide to the OCORA Core team a PDF extract of his/her Polarion artifact.

1. Open the "Export to PDF" pop-up

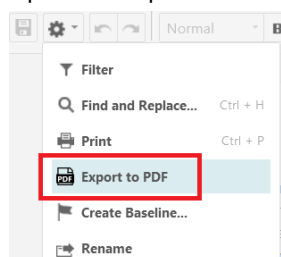


Figure 7 PDF extract for Polarion artifacts

2. Fill the pop-up with this information

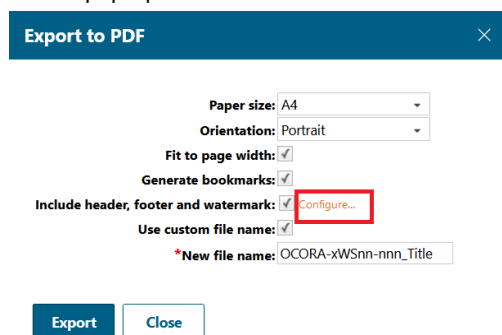


Figure 8 Extract to PDF pop-up

note: the "New file name" corresponds to the *file.pdf* name

3. Select "configure":

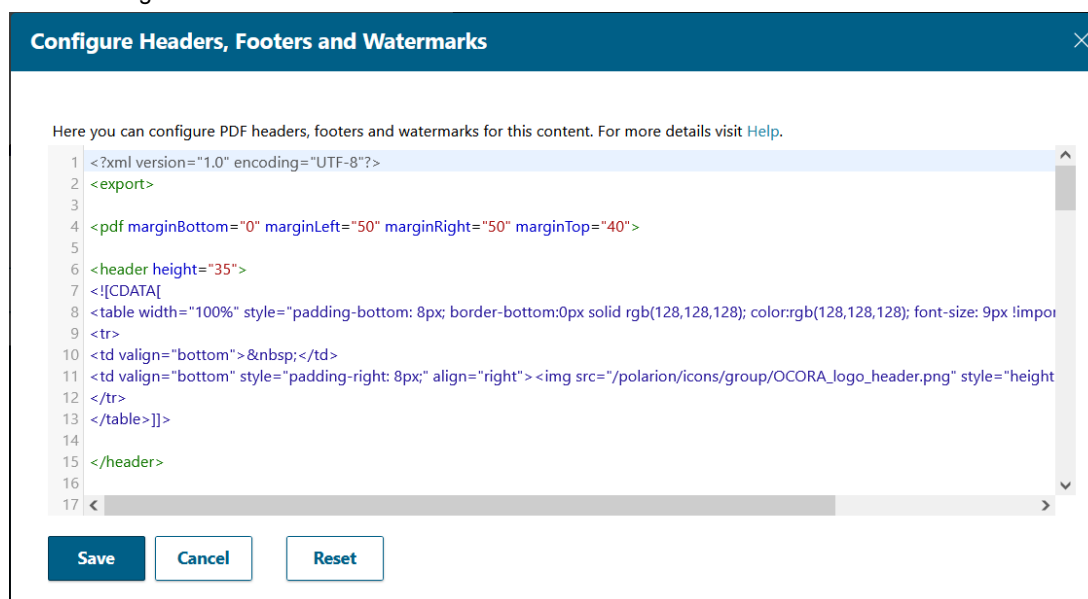


Figure 9 "Configure" PDF pop-up

4. Fill this pop-up with the following data:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<export>
```

```
<pdf marginBottom="0" marginLeft="50" marginRight="50" marginTop="40">
```

```
<header height="35">
```

```
<![CDATA[
```

```
<table width="100%" style="padding-bottom: 8px; border-bottom:0px solid rgb(128,128,128);
color:rgb(128,128,128); font-size: 9px !important; margin-bottom: 20px;">
```

```
<tr>
```

```
<td valign="bottom">&nbsp;</td>
```

```
<td valign="bottom" style="padding-right: 8px;" align="right"></td>
```

```
</tr>
```

```
</table>]]>
```

```
</header>
```

```
<footer height="25" scope="1">
```

```
<![CDATA[
```

```
]]>
```

```
</footer>
```

```
<footer height="25">
```

```
<![CDATA[
```

```
<table width="100%" style="border-top:0px solid rgb(128,128,128); color:rgb(128,128,128); font-size: 13px
!important;background-color:#e8eae9;">
```

```
<tr>
```

```

<td width="2%" align="left"></td>
<td width="20%" align="left">${docID}</td>
<td width="46%" align="center">v${docVersion} (Rev${revision}) / ${convDate}</td>
<td width="20%" align="right" padding-top="8px" padding-bottom="8px"></td>
<td width="10%" align="right">${page}/${total}</td>
<td width="2%" align="left"></td>
</tr>
</table>]]>

</footer>

</pdf>

<pdf-compare marginBottom="10" marginLeft="10" marginRight="10" marginTop="10">

<header height="35">
<![CDATA[
<table width="100%" style="color:rgb(128,128,128); font-size: 9px !important; margin-bottom: 20px;">
<tr>
<td width="30%"></td>
<td width="70%" align="right">${projectName}<br>${documentTitle} (compare rev. ${revision1} and
${revision2})</td>
</tr>
</table>]]>

</header>

<footer height="25">
<![CDATA[
<table width="100%" style="border-top:1px solid rgb(128,128,128); color:rgb(128,128,128); font-size: 9px
!important;">
<tr>
<td width="20%"><span style="color:rgb(0,0,0);">${page}/${total}</span></td>
<td width="60%" align="center"><a style="color:rgb(128,128,128); font-size: 8px !important;"><!-- SBB CFF FFS //--
></a></td>
<td width="20%" align="right">${generated}</td>
</tr>
</table>]]>

</footer>

</pdf-compare>

<pdf-compare-documents marginBottom="10" marginLeft="10" marginRight="10" marginTop="10">

<header height="35">
<![CDATA[
<table width="100%" style="color:rgb(128,128,128); font-size: 9px !important; margin-bottom: 20px;">

```

```

<tr>
<td width="30%"></td>
<td width="70%" align="right">${projectName1}<br>${documentTitle1} rev. ${revision1} compare ${projectName2}
${documentTitle2} rev. ${revision2}</td>
</tr>
</table><br>&nbsp;]]>

</header>

<footer height="25">
<![CDATA[
<table width="100%" style="border-top:1px solid rgb(128,128,128); color:rgb(128,128,128); font-size: 9px
!important;">
<tr>
<td width="20%"><span style="color:rgb(0,0,0);">${page}/${total}</span></td>
<td width="60%" align="center"><a style="color:rgb(128,128,128); font-size: 8px !important;"><!-- SBB CFF FFS //--
></a></td>
<td width="20%" align="right">${generated}</td>
</tr>
</table>]]>

</footer>

</pdf-compare-documents>

</export>

```

5. Click "Save" and "Export" the PDF.

3.3.5 Documentation maintenance

The maintenance of the OCORA documentation has different aspects, depending of the origin of the reviewer and the storage of the document:

The relevant reviewers (i.e. people of the WS where the artifact is produced))with their relevant sections to analyse (if appropriate) shall be mentioned into the OCORA-BWS00-010_Documentation_Plan for each artifact.

The QRAMSS manager shall check that before each artifact official delivery, a review sheet is available from each relevant reviewer and all comments are resolved.

Each reviewer shall provide to the artifact author a set of comments :

1. Each reviewer shall provide to the document's author a set of comments thanks to "comments" functionality of Polarion
2. The author shall answer the comments and update the artifact accordingly if necessary,
3. Each reviewer shall close its comments before allowing the release of the document,
4. When all comments are closed, including the ones from the CORE team, the author shall provide to the core team a final version of the document with all comments accepted.

This concerns only the documentation created with Microsoft Office:

1. Each reviewer shall provide to the document's author a set of comments thanks to Microsoft Office "comments"

functionality,

2. Track changes shall be used by the authors when updated a draft version of a document,
3. Track changes shall be visible until the final draft of the document as well as the answers to the comments,
4. Each reviewer shall close its comments before allowing the release of the document,
5. When all comments are closed, including the ones from the CORE team, the author shall provide to the core team a final version of the document with all track changes and comments accepted.

Add in the introduction part of each document a brief description of the OCORA documentation maintenance (i.e. future change process management). This section must be added when in the first release of OCORA that will be officially shared with external reviewers. Thus, external reviewers understand the way they can request modifications of a document for a further OCORA release.

Each external reviewer of OCORA shall use to [\[OCORA-BWS01-040\] – Feedback Form](#) to provide comment to the OCORA initiative on one of its deliverables.

3.3.6 Documentation control sheet

To ensure that the documentation of the OCORA Program is still in line with the expectations presented above, quality checkpoints based on a Control Sheet (to be set-up in future release) shall be performed before ending by a QRAMSS manager:

- an OCORA release (e.g. R3),
- a CENELEC phase (i.e. from 2 to 5).

The OCORA planning shall content a QRAMSS checkpoints of all documentation before each OCORA release delivery.

A checklist defines the "quality" aspects to be checked before releasing a document such as:

- Versioning rules respects (0.01 -> 0.02...)
- Comments resolved by reviewer
- Review files stored under the common database
- Latest template applicable used
- English language used
- Name of the document coherent with the projekt and the content
- ID for the document available and correct regarding documents management
- Correct date for creation, review and release
- Updated revision history and coherent between dates/version/remarks?
- All the applicable "Workstream definition" fields are fulfilled
- Review and release of the document by competent persons, in accordance with the allocation of Roles

3.4 Requirement management

The rules for managing requirement in Polarion are defined in the [\[OCORA-TWS05-010\] – Requirements – Management Guideline.](#)

3.5 Configuration Management

OCORA documentation is organised in "releases" which are published into GitHub as public documentation. This is performed twice a year.

The working documents and other artifacts are either:

- stored under SharePoint with using its own configuration management (i.e. availability of historical version),
- created and managed under Polarion which owns a dedicated management of historical versions.

3.6 Change Management

OCORA initiative is only creating paper work, which means that no dedicated change management tool such as Change Request database is mandatory. It may be set-up in a future release of OCORA if considered as relevant. From now, the strategy presented in [OCORA-8025 - Documentation maintenance](#) applicable.

3.7 Tool Management

The management of the tools used in by the OCORA initiative is presented in [\[OCORA-BWS08-020\] - Tooling](#).

3.8 Organization and Responsibilities

EN 50129 [A4] requires that activities shall be divided in:

- Design and Implementation including Specification, Design, Manufacturing and Installation (DI);
- Verification, including phases Verification and overall requirements Validation, Test and Commissioning (VER);
- Validation, including Safety Analyses and Safety Verification and Validation (VAL);
- Assessment (ASSR).

This kind of formal assignment is not relevant for the OCORA initiative as it focuses on specification level and is not a legal structure. However, the main idea of the CENELEC independence of roles is nevertheless kept into OCORA. Indeed, the TWS07 (and formally TWS09) dealing with RAMS activities can be considered as filling the roles of VER and VAL activities with some tailored elements focussed on the limited activities of OCORA. The PM role can be assimilated to the OCORA CORE team with some tailored items and the other workstreams (e.g. TW01 - Architecture) can be assimilated to the design role (i.e. DI). It is intended when phase 4 will be reached the the OCORA documentation will be submitted to an external ISA (i.e. ASSR according to CENELEC roles) for an external opinion. However, no formal accreditation nor certificated is expected.

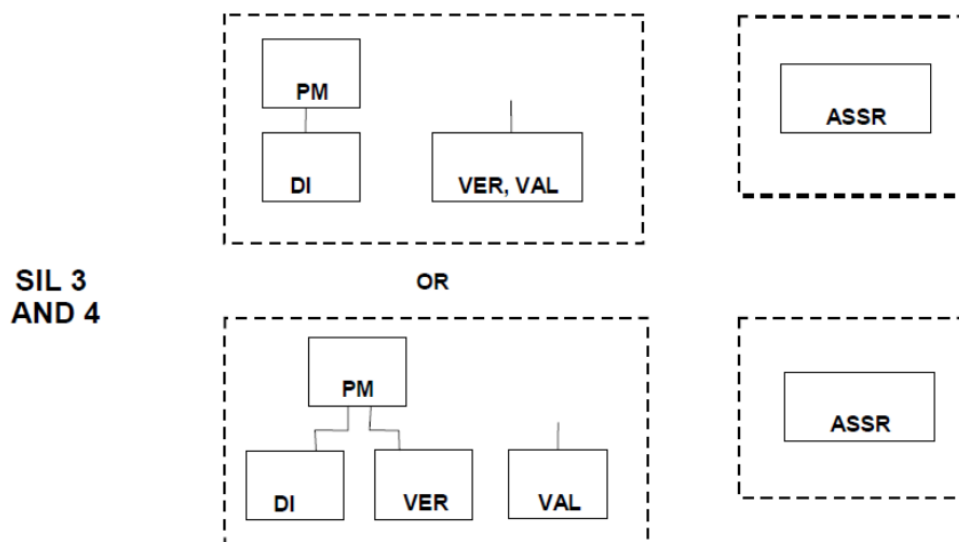


Figure 10 CENELEC Arrangement for independence

The following Table 6 defines the role, the name and the description of responsibilities of the roles involved in OCORA as presented on the figure above.


Role	Name	Responsibilities
CORE Team (PM)	Albert Ledermann SBB Rolf Mühlemann SBB Jack Schneider SBB Stéphane Callet SNCF Etienne Kuntzel SNCF Jérôme Lalouette SNCF Patrick Marsch DB Baseliyos Jacob DB Matthias Moritz DB Joost van Gennip NS Pieter Vreeswijk NS Markus Mandlmayr ÖBB	Manage Program until contract closure, respecting the [OCORA-BWS07-010] - Alliances . Responsible for providing the necessary means and budget for the staffing of OCORA activities. Define the project planning (i.e. dates and deliverables) for each OCORA release. Releasing the content of each OCORA delivery release. Communicate about OCORA into other European organisation (e.g. ERJU, UNIFE).
Architects and Designers (DI)	TWS01 TWS04 TWS05 TWS08	Develop and deliver the OCORA set of requirements for call for tenders in line with the [OCORA-BWS05-010] - Road Map and as agreed with the CORE Team:
RAMSS engineers (VER & VAL)	Up to R3 members of the TWS07 and TWS06 team From R4: only TWS07 for RAMS (without cyber-security)	Implement the project management defined by OCORA BWSxx. RAMSS engineers are responsible: <ul style="list-style-type: none"> to deploy RAMSS Process, Method and Tools in accordance to existing standards and regulations and propose improvements based on REX (Return on Experience) to a modular architecture; to perform RAMSS analysis, manage Hazard Log, Threat Log, review artifacts of other OCORA WS from a RAMSS perspective; to build the documentation of the CENELEC V-Cycle up to the Design Safety and cyber-security Case in Phase 5; to apply the safety and cyber-security assurance methodologies (risk acceptance criteria, safety and cyber-security analyses, verification and validation) defined by TWS07 and TWS06; to defend RAMSS argumentations in front of internal and external reviewers (including potential ISA); to define and follow-up action plans to close the findings of the assessor's informal opinion (if any) <div>OCORA-10173 - No more cyber-security team in OCORA</div>
Testing engineers (VER)	Up to R3: Members of the TWS09 team From R4: Not allocated	Define global verification strategy (i.e. testing part) and produces Test Plan, ensuring consistency of testing activities; synchronize testing activities along the OCORA V-cycle and review artifacts of other OCORA WS from a testing perspective; <div>OCORA-10171 - No more Testing activities in OCORA</div>
Quality Manager (QM)	CORE Team / TWS07	Ensure  OCORA-7939 - Framework for QRAMSS Management application, supporting the CORE team to prepare OCORA Release deliveries. Control project deliverables compliance through inspection and checkpoints in planning. <div>OCORA-10172 - No quality team for OCORA</div>

Table 1 Responsibilities

3.9 Limits of Responsibility

The OCORA initiative is responsible for providing relevant and complete set of requirements for future call for tenders to build modular CCS OB. Its responsibility is limited to:

- the highest possible level of quality and maturity for these deliverables including potential future revisions,
- ensure the absence of conflicts with any standard or directive dealing with interoperability (e.g. SUBSET-026).

OCORA is not developing any product (e.g. hardware, software) or project (e.g. retrofit of a complete train fleet with new OCORA CCS OB) and therefore has no responsibility is potential erroneous implementation of the OCORA set of requirements by a supplier or RU.

3.10 Operation and maintenance

Operation and maintenance phase (i.e. Phase 11 of the CENELEC C-cycle are handled by the RU and involves:

- the RU themselves with all internal teams,
- the different building blocks suppliers (e.g. for building block updates, new equipments)
- the different stakeholders identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) (e.g. CCS OB integrator) when they don't belong to one of the above category.

The participation of the OCORA initiative to this phase is presented in [OCORA-8652 - OCORA initiative](#).

3.11 Decommissioning and disposal

This phase is out of scope for OCORA as defined in [OCORA-8651 - OCORA initiative](#).

4 Safety Activities

The OCORA Program is handled by the collaboration of members having signed the MEMORANDUM OF UNDERSTANDING [64]. Up to OCORA R3, five companies are part of this collaboration: DB AG, SNCF, SBB, NS and ÖBB.

The OCORA Program does not intend to develop the full V cycle according to EN 50126-1 [66]. It aims at defining a future reference architecture to build CCS OB system based on a modular way. This is fully explained in [10]. This strategy leads to apply the first 5 phases of the V cycle within OCORA Program whereas the others will be realised by the suppliers. This strategy is presented in the System Concept [57] and recapped hereafter.

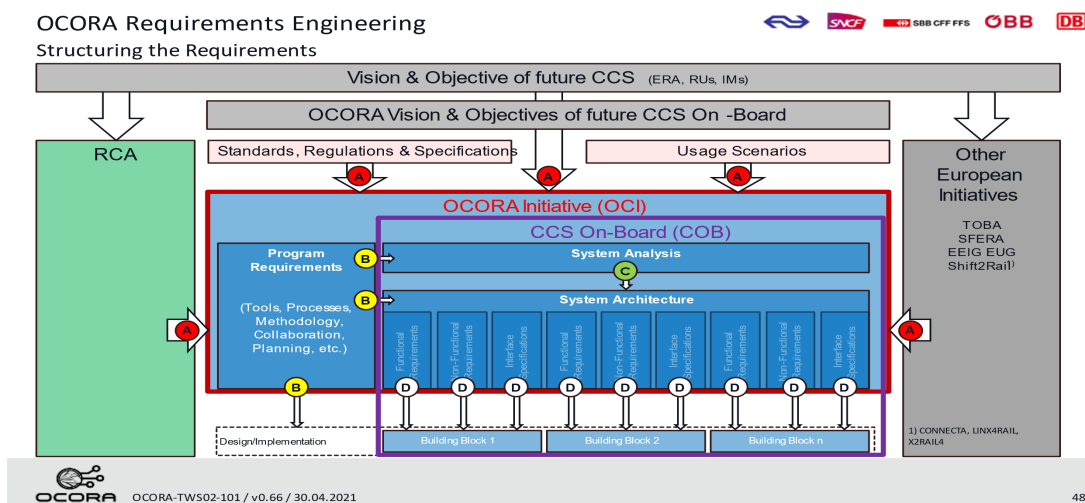


Figure 11 OCORA Requirements Structure from Project Input Sources

The aim of the OCORA Program is to provide the D Level requirements from Figure 1 which will be used to create the call for tenders to order the different building blocks types composing an OCORA compliant CCS OB system (refer to §2.2).

The delivery of these D Level requirements is correlated to the end of Phase 5 from the EN 50126-1 [66] V cycle, as presented on Figure 3.

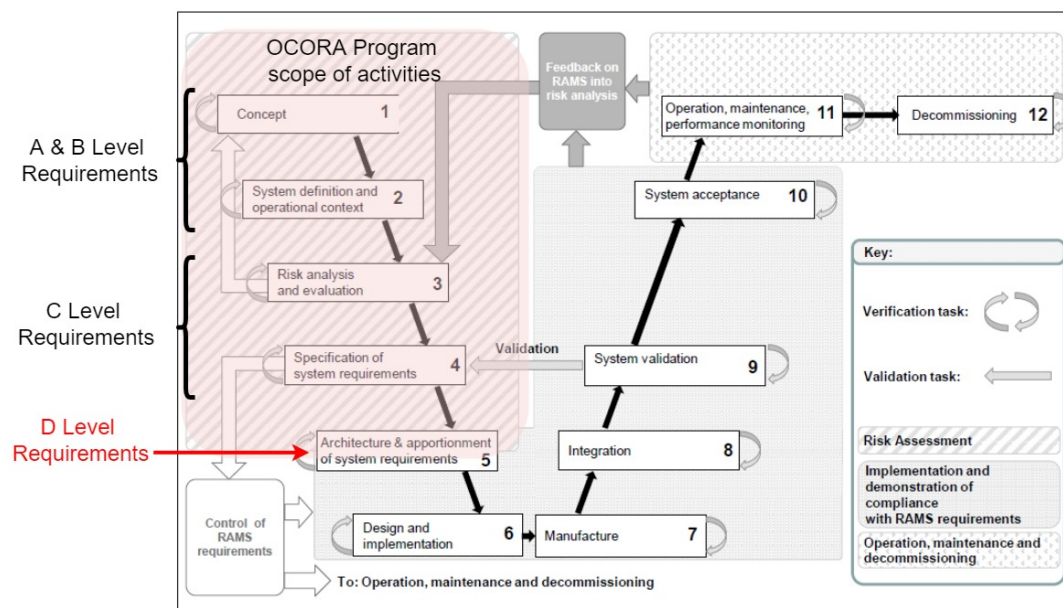


Figure 12 OCORA requirements in the V cycle

The present QRAMSS plans covers the quality, RAM, safety and cyber-security activities for the first 5 phase of the OCORA program. At the end of Phase 5, OCORA is expected to provide documentation to be used in future call for tenders. Phases 6 to 10 will be developed by the manufacturers, based on the "D level requirements" provided as input under a similar format as the current TSI CCS SUBSETS. Finally, phases 11 and 12 will be handled by the RU's that ordered OCORA compliant products with the support of the manufacturers who will provided several evolutions activities

during the Building Blocks' lifetime (refer to [\[OCORA-TWS07-020\] - RAMS Evolution management](#)). However, OCORA intends to support all stakeholders identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) with safety documentation adapted to a modular architecture. This is defined from [OCORA-8617 - Phase 8 "Integration"](#) to [OCORA-8624 - Phase 11 "Operation, maintenance and performance monitoring"](#).

To meet the objectives laid down in the [\[OCORA-TWS07-010\] - Modular Safety – Strategy](#) and in the [\[OCORA-TWS05-020\] – Stakeholder Requirements](#), any new Building Block defined by OCORA D level requirements shall be designed, procured and commissioned so that it can be used and maintained at an overall level of safety that is at least equivalent to the overall level of safety of existing Products offering comparable services or functions.

To achieve it:

- New components shall be developed following complete lifecycles, from requirements specification to requirements tests. Along the phases of these lifecycles, safety analysis, validations and verifications shall be carried out to ensure that components meet expected requirements.
- Similarly, any change to a component shall be specified, designed, procured and commissioned in such a way that it can be used and maintained at an overall level of safety that is at least equivalent to the overall level of existing solutions offering comparable services or functions.

This OCORA QRAMSS Plan comprises activities to be executed during the first five applicable lifecycle phases according to [\[EN 50126-1:2017-10\] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety \(RAMS\) - Part 1: Generic RAMS Process](#). The safety goals of OCORA are:

- to identify hazard and assign feared events with a dedicated TFFR value to the different OCORA Building Blocks functionalities. This activity will be initiated into the PRAMS domain of ERJU and the results will be used by OCORA;
- to provide a set of safety requirements to the OCORA Building Blocks to be used in the future call for tenders;
- to identify generic SRAC for all Building Blocks (refer to [\[OCORA-TWS07-030\] - RAMS SRAC-AC Management](#));
- to provide new methodologies for evolution management during the Building Blocks' lifetime and integrated CCS-OB systems (refer to [\[OCORA-TWS07-020\] - RAMS Evolution management](#));
- to define a optimized approval process for Generic Applications and Specific Application integrating OCORA Building Blocks (refer to [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#));
- to support the remote configuration management process for OCORA Building Blocks (refer to [\[OCORA-TWS07-060\] - Configuration Management Concept](#))

To reach these goals a set of safety activities have been defined at every phase of OCORA development.

4.1 Safety Management

4.1.1 Safety Planning

The basis for the Safety management is the present QRAMSS Plan, which defines the organization, the processes and the activities that will be in operation. The present plan will be used to define and schedule the tasks of the safety program and to allocate these tasks among members of the RAMS team.

It is not possible to directly map OCORA releases into the CENELEC V-cycle as each release work on parallel sub-systems of OCORA with different maturity level. Therefore, the safety planning is limited to the current release, split into the different sub-systems identified into the [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#).

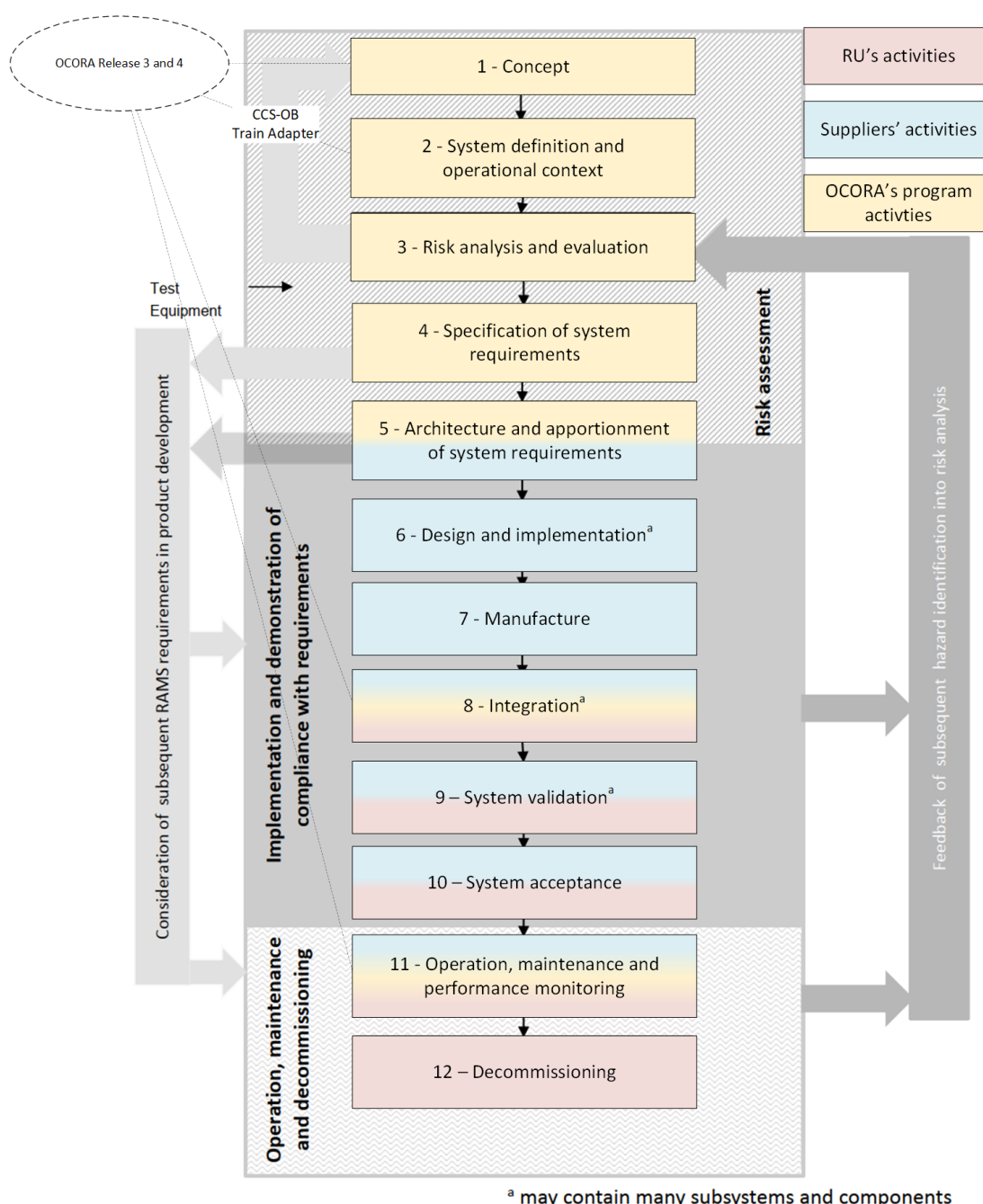


Figure 13 OCORA Releases into the V-cycle

The detailed safety deliverables to be provided for each phase is presented in the following sub-sections.

4.1.2 Hazard Log management

The aim of the Hazard Log (HZL) is to record in a single report all the hazards identified (by safety studies, reviews, V&V, ...). It provides also a progress status for the closure of each hazard, with reference to documented evidences. The Hazard Log (HZL) must be updated by the SM at each step of the lifecycle of the system and is released periodically to summarize the hazards status.

At the end of the development, the Hazard Log must ensure that all the entries have been closed and this is possible only if there is evidence that:

- The residual risk related to the hazard is negligible and the safety requirements related to the hazard have been implemented and verified;

OR

- The safety requirements related to the hazard are exported outside the scope of the developments as safety-related application conditions (and communicated/agreed with relevant stakeholders).

So far, the Hazard Log has not been initiated by the safety team. This is under control most hazards are known for the CCS OB system and consigned in the [\[SUBSET-091\]](#). A proper risks analysis with potential new hazards will be performed for new functionalities presented in [OCORA-7936 - Architecture](#) where no specifications exist yet.

4.1.3 Model Based Safety Analysis

Capella is a MBSE tool based on the Arcadia method. Capella is used in the OCORA program in order to enhance communication

among stakeholders. It supports the architecture and design activities. It also ensures the coherence and completeness of the

architecture. This is presented in [\[OCORA-TWS01-041\] - MBSE-Modelling-Guideline](#).

The MBSE structure can be linked to the CENELEC V cycle of EN 50126-1 as presented below.

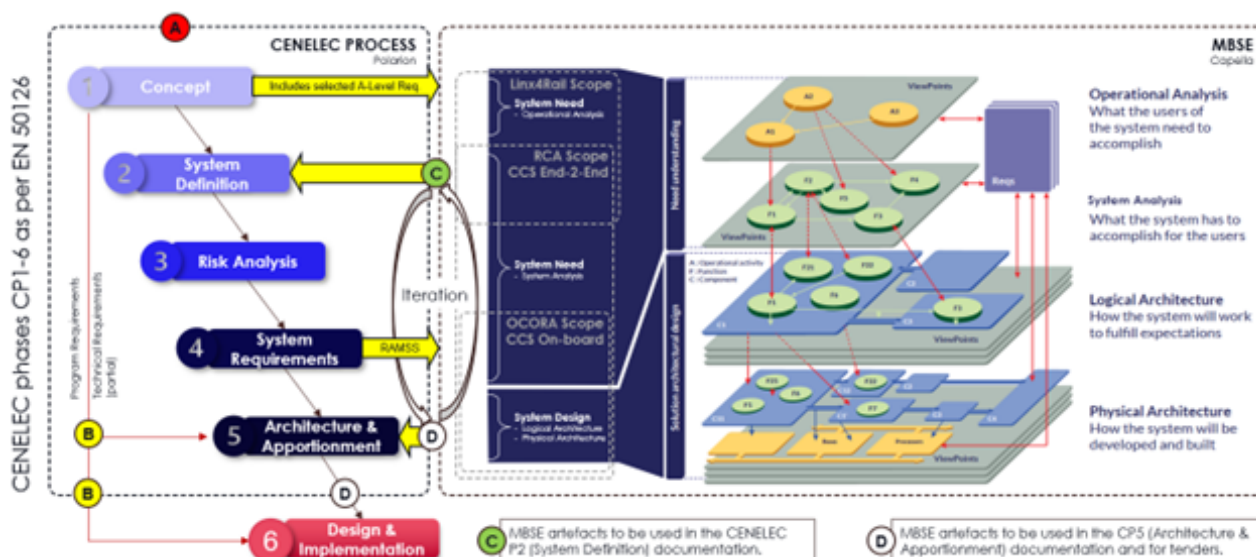


Figure 14 MBSE structure in EN 50126 V cycle

The use of a MBSE implies that safety analyses are adapted to the artifacts provided by the model. They are presented in the following sections.

4.2 Overall OCORA Lifecycle

The term safety analysis covers all the activities whose aim is to evaluate (qualitatively and quantitatively) and provide evidence of the safety of a system.

Every safety analysis shall produce a report and the identified hazards, together with associated safety requirements, shall be logged in the hazard log.

The OCORA lifecycle and the related documentation is shown on the above picture.

4.3 Phase 1 "Concept"

4.3.1 Objective

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

The objective of this phase is to develop a sufficient understanding of the system to ensure a proper performance of all subsequent RAMS life cycle activities.

4.3.2 Activities

In the context of RAMS performance, the following aspects should be analysed:

a) the scope, context and purpose of the system;

b) the environment of the system, including:

– physical issues;

– system interface issues;

– legislative and economic issues (if they can have impact).

c) previous RAMS requirements and past RAMS performance of similar and/or related systems;

d) current RAMS policy and targets of the relevant railway duty holders;

e) safety legislation.

The scope of the RAMS management requirements for subsequent system life cycle RAMS tasks shall be defined.

4.3.2.1 OCORA initiative

The OCORA initiative shall create an OCORA System Concept that covers the complete OCORA CCS OB system.

This is covered by [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#).

4.3.2.2 Building Blocks suppliers

Each BB supplier shall create its own System Concept for its building block in conformity with EN 50126 and OCORA set of requirements for this building block.

4.3.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) shall create its own System Concept for its integration level in conformity with EN 50126 and OCORA requirements for this integrator.

4.3.2.4 Railway Undertakings

Each RU shall create its own System Concept for its project in conformity with EN 50126 and OCORA set of requirements for system level.

4.4 Phase 2 “System Definition and Operational Context”

4.4.1 Objective

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

The objectives of this life cycle phase are:

- a) define the system and its mission profile;*
- b) define the boundary of the system;*
- c) establish the operational requirements influencing the characteristics of the system;*
- d) define the scope of system risk analysis;*
- e) establish the initial RAM plan for the system;*
- f) establish the initial Safety plan for the System;*
- g) define the functions to be provided by the system;*
- h) define the organisation for RAM and safety management of the system as far as they affect the potential RAMS performance of the system.*

4.4.2 Activities

4.4.2.1 OCORA initiative

4.4.2.1.1 QRAMSS Plan

The aim of this activity is to establish a RAMSS Plan compliant to EN50126, EN50128, EN50657, EN50129 and TS50701 with agreed tailored rules.

This plan includes or reference documentation for verifying that each phase of the lifecycle satisfies the specific RAMSS requirements identified in the previous phase.

4.4.2.1.2 MBSA - Operational Safety Analysis

The OCORA Safety team is in charge of realising a preliminary safety analysis based on the Operational Analysis realised in Capella and part of the MBSE model.

This analysis is conducted using inductive/deductive methods (e.g. hazard list or breakdown structure, STPA, ...). Starting from the operational context/procedures and the defined system functions, it aims at:

- identifying the hazards at the boundary of the system under consideration (resulting from the use of the system in a specified context, as defined in the system specification);
- classifying the consequences (possible accidents) of these hazards;
- identifying the necessary mitigations for the system or the elements of the system (including preliminary SIL allocation to functions), to lower the risk to an acceptable level;
- (optional) predict Hazardous Failure Rate (HFR) achievable (to be confirmed by FTA or equivalent method after detailed design).

The details of the way to perform this analysis will be defined in a future release of OCORA. The methodology will be defined by the PRAMS Team of the ERJU project into a Safety Guideline where most of TWS07 members are involved.

4.4.2.1.3 System Definition

The aim of this activity is to properly provide the first stones to the SuC. The OCORA program is using a template built from EN 50126-1 and 2 and will cover different SuC as presented in the [\[OCORA-TWS07-100\] – CENELEC Phase 1 – System Concept](#). So far, its realisation is on hold because of topics transition between OCORA and ERJU. Therefore, the creation of 2 levels of System Definition (i.e. whole CCS OB at top level and then one for each building block) will be reevaluated for R5 (refer to [OCORA-10204 - System Definition to create](#)).

4.4.2.2 Building Blocks suppliers

Each BB supplier shall provide all deliverables expected for EN 50126 Phase 2 and be conform to OCORA set of requirements for this building block (e.g. use of tool allowing to integrate the OCORA MBSE models).

These requirements will be defined in future release of OCORA and later in the project development.

4.4.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) provide all deliverables expected for EN 50126 Phase 2 and be conform to OCORA set of requirements for this integration level.

These requirements will be defined in future release of OCORA and later in the project development.

4.4.2.4 Railway Undertakings

Each RU shall provide all deliverables expected for EN 50126 Phase 2 and be conform to OCORA set of requirements for the system level.

These requirements will be defined in future release of OCORA and later in the project development.

4.5 Phase 3 “Risk Analysis and Evaluation”

4.5.1 Objective

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

The objectives of this life cycle phase are to:

- a) *identify and classify hazards / RAM equivalents associated with the system;*
- b) *select risk acceptance principles (RAP);*
- c) *define and apply risk acceptance criteria (RAC);*
- d) *assess risks;*
- e) *establish a process for on-going risk management.*

NOTE RAM equivalent to hazard is a condition that could lead to commercial loss related to RAM.

For the reason of simplification, the life cycle representation in this standard shows risk analysis as a one time activity in the early stage of a project. At this stage, for some aspects of the risk analysis only estimations can be made because the detailed design of the product, system or process is not yet available and analysed. This early risk analysis serves as a basis for defining the risk based RAMS system requirements (see life cycle phase 4, 7.5).

Afterwards, an on-going risk management shall be conducted in order to make sure that the risks associated with the system, subsystem, equipment are controlled.

Any analysis produced during the process should include or refer to:

- 1) *the limits of any analysis carried out;*
- 2) *assumptions made during the analysis;*
- 3) *confidence limits applying to data used within the analysis;*
- 4) *the methods, tool and techniques used.*

4.5.2 Activities

4.5.2.1 OCORA initiative

4.5.2.1.1 Risk Analysis

The definition of safety requirements is carried out following a risk-based approach and the first activity of the Safety Plan to be carried out is the risk analysis (including hazard identification).

The methodology used for risk analysis uses typically a FMEA approach and related methodology is described below.

For every function and interface, deviations that may become hazards for the system are identified. For each hazard, the causes and their final consequences on the railway system and its users are traced in a top-down manner.

An initial risk level is assigned to each hazard through the consideration of the frequency of occurrence of the hazard [Table 2] and the evaluation of the consequence for people and environment [Table 3] using a "Frequency vs consequence" matrix [Table 4], defined according to the guidance provided in EN50126 and related Risk Acceptance Matrix.

Category	Description	Example of frequency range (based on a single item operating 24 h/day)
A Frequent	Likely to occur frequently. The hazard will be continually experienced	more than once within a period of approximately 6 weeks
B Probable	Will occur several times. The hazard can be expected to occur often.	approximately once per 6 weeks to once per year
C Occasional	Likely to occur several times. The hazard can be expected to occur several times.	approximately once per 1 year to once per 10 years
D Rare	Likely to occur sometime in the system life cycle. The hazard can reasonably expect to occur.	approximately once per 10 years to once per 1 000 years
E Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.	approximately once per 1 000 years to once per 100 000 years
F Highly improbable	Extremely unlikely to occur. It can be assumed that the hazard may not occur.	once in a period of approximately 100 000 years or more

Table 2 Frequency of Occurrence Classification

Hazard Category	Consequence for people and environment	Consequence for Service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment	
Critical	Single fatality and/or several injury and/or significant damage to the environment.	Loss of major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

Table 3 Hazard Severity Level

	Severity levels of hazard Consequence			
	4: Insignificant	3: Marginal	2: Critical	1: Catastrophic
A: Frequent	Undesirable	Intolerable	Intolerable	Intolerable

	Severity levels of hazard Consequence			
B: Probable	Tolerable	Undesirable	Intolerable	Intolerable
C: Occasional	Tolerable	Undesirable	Undesirable	Intolerable
D: Rare	Negligible	Tolerable	Undesirable	Undesirable
E: Improbable	Negligible	Negligible	Tolerable	Undesirable
F: Highly improbable	Negligible	Negligible	Negligible	Tolerable

Table 4 Risk Evaluation and Acceptance

This matrix is used to define the initial risk assessment associated to the occurrence of the identified hazards. The applied Qualitative Risk Categories are summarized in the following Table 5.

Risk Level	Actions to be applied against each category
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority
Tolerable	Acceptable with adequate control and the agreement of the Railway Authority
Negligible	Acceptable with/without any agreement of the Railway Authority

Table 5 Qualitative Risk Categories

When risk is assessed as higher than negligible it is mandatory to identify all the safety requirements necessary to reduce the associated risk.

When the risk assessment is negligible (or the event eliminated, e.g. by inherent fail-safe characteristics), it won't be necessary to define any new safety requirement.

After defining the safety requirements, a re-assessment of the risk is performed using Table 4 to determine the final risk assessment.

In case during the final risk assessment stage of a hazardous event it would not be possible to reduce the risk to a tolerable level, the involved hazard and its associated residual risk, shall be communicated by means of the hazard log report (or by means of a dedicated SRAC document) and agreed with the user.

4.5.2.1.2 Hazard Log

The OCORA Hazard Log will be created based on the hazards list coming from [SUBSET-091] in a future release of OCORA. Additional hazards may be added depending on the results of OCORA-7941 - Risk Analysis. It provides a progress status for the closure of each hazard and related safety requirements (including SRACs), with reference to documented evidences at any stage in the development life-cycle. It must be noticed that in the OCORA program, the OCORA Hazard Log will end at the end of Phase 5, meaning the design phase (including SRAC). However, the evidence of correct fulfillment of each hazard relies on the responsibility of each stakeholder involved in a OCORA compliant product or project. Each hazard identified as applicable to the OCORA program shall have the following attributes:

- Identification number;
- Source document from which the hazard has been raised;
- Potential accident that can result from the hazard;
- Hazardous situation that can lead to the potential accident;
- Hazard Cause;
- Severity of the consequence of the accident;
- Frequency of occurrence of the hazardous situation taking into account the identified mitigations.

Then for each OCORA safety requirement the following attributes shall be recorded:

- Unique reference number of the safety requirement within the hazard log;
- Text of the safety requirement needed for hazard elimination or risk mitigation;
- Entity or process in charge of the implementation of the requirement (i.e. OCORA stakeholders);

- Evidences of the implementation of the safety requirement that are necessary to reach the subsequent closure status at design level (i.e. testings measure(s) provided by the OCORA TWS09 Team);
- Closure status at design level of the safety requirement.

Traceability of OCORA safety requirements against hazards is also recorded in the OCORA Hazard Log.

4.6 Phase 4 “Specification of System Requirements”

4.6.1 Objective

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

The objectives of this life cycle phase are to:

- a) specify the overall RAMS requirements for the system under consideration;*
- b) specify the overall demonstration process and criteria for acceptance of RAMS of the system;*
- c) provide a comprehensive and identified set of requirements for the subsequent life cycle phases;*
- d) specify necessary monitoring requirements according to the process for analysing operation and maintenance performance arranged in the Safety Plan (that enable the system to perform the required tasks in life cycle phase 11).*

4.6.2 Activities

4.6.2.1 OCORA initiative

4.6.2.1.1 MBSA - System Hazard Analysis

The OCORA Safety team performs the safety hazard analysis at functional level. The latter will take as input the hazards list issued from [OCORA-7976 - Hazard Log](#) and applied to the Capella artifact corresponding to the "System Analysis". This analysis will be performed using a FMEA method. It aims at:

- identifying the cause and consequences of the failures of the functions supported by the system/product;
- identifying the mitigations necessary to control the hazards and to lower the risk at an acceptable level;
- confirming the SIL allocation to the elements of the system.

The details of the way to perform this analysis will be defined in a future release of OCORA. The methodology (e.g. FMEA) will be defined by the PRAMS Team of the ERJU project into a Safety Guideline where most of TWS07 members are involved.

4.6.2.1.2 OCORA Safety requirements

The TWS07 Team shall provide at the end of Phase 4 a complete list of safety requirements applicable at System Level (i.e. CCS OB). The latter shall then be integrated in the [OCORA-7976 - Hazard Log](#) and traced with the OCORA hazards.

Each function defined in the Capella model and analysed as safety critical shall get its own TFFR, in accordance with [\[SU BSET-091\]](#) overall target(s).

At this step of the OCORA program, no safety requirements at building block level is expected.

The OCORA safety requirements shall respect the rules defined in [\[OCORA-TWS05-010\] – Requirements – Management Guideline](#).

4.6.2.1.3 Independent Safety Assessment

The OCORA initiative may require an informal opinion from an ISA when the level of requirements and processes is judged as mature enough. The scope of this activity would be to realise the "*Validation Report covering phases 1 to 4*" required by EN 50126 in Phase 4.

This is not planned up to OCORA R4.

4.6.2.2 Building Blocks suppliers

Each BB supplier shall provide all deliverables expected for EN 50126 Phase 4 and be conform to OCORA set of requirements for this building block (e.g. use of tool allowing to integrate the OCORA MBSE models).

These requirements will be defined in future release of OCORA and later in the project development.

4.6.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) provide all deliverables expected for EN 50126 Phase 4 and be conform to OCORA set of requirements for this integration level. This phase will provide crucial requirements in particular to the CCS OB Builder (refer to [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) for details) who will be responsible for the OCORA CCS OB safety demonstration (i.e. scope of the actual TSI CCS TSI CCS: 02016R0919).

These requirements will be defined in future release of OCORA and later in the project development.

4.6.2.4 Railway Undertakings

Each RU shall provide all deliverables expected for EN 50126 Phase 4 and be conform to OCORA set of requirements for the system level.

These requirements will be defined in future release of OCORA and later in the project development.

4.7 Phase 5 "Architecture and apportionment of system requirements"

4.7.1 Objective

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

The objectives of this life cycle phase are to:

- a) apportion the system RAMS requirements to the designated subsystems and/or components;*
- b) design subsystems and components that work together as a system which fulfils the required functions at the system level;*
- c) describe the RAMS requirements and specify the interfaces for all subsystems and components derived from the RAMS requirements (which prepares later integration activities);*
- d) define the acceptance criteria to demonstrate fulfilment of the RAMS requirements for the system, subsystem, equipment in subsequent lifecycle phases;*
- e) identify and evaluate the significance of the interactions between the subsystems.*

This phase is the most critical one because it represents the border between the OCORA Project and all stakeholders defined in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#).

4.7.2 Activities

4.7.2.1 OCORA initiative

4.7.2.1.1 Interface Hazard Analysis

This step focuses on the architecture models of Capella. For safety purpose, only the physical is relevant. Indeed, the logical architecture is an intermediate design phase where the physical elements are not yet defined whereas only the physical architecture is expected by EN 50126 for Phase 5. At this step, EN 50126 requires that an interface hazard analysis is performed to identify the safety critical ones. This analysis is performed using a FMEA method. It aims at:

- identifying the cause and consequences of the failures of the interfaces supported by the CCS OB/building block;
- identifying the mitigations necessary to control the hazards and to lower the risk at an acceptable level;
- confirming the SIL allocation to each building block.

The details of the way to perform this interface analysis will be defined in a future release of OCORA. The methodology (e.g. FMEA) will be defined by the PRAMS Team of the ERJU project into a Safety Guideline where most of TWS07 members are involved.

4.7.2.1.2 Fault tree analysis

This analysis aims to gather and link the causes leading to each hazard identified at the boundary of the system (identifying the complete list of multiple faults scenarios leading to an hazard of the [OCORA-7976 - Hazard Log](#)). It is also used to quantify the safety target achieved by the OCORA assigning the failure rates to the different causes/Hw faults.

The latter is build according to the Physical Architecture of the Capella model and to the TFFR targets defined in [OCOR A-10223 - OCORA Safety requirements](#).

The details of the way to perform this FTA will be defined in a future release of OCORA. The methodology will be defined by the PRAMS Team of the ERJU project into a Safety Guideline where most of TWS07 members are involved.

4.7.2.1.3 OCORA Safety requirements

The TWS07 Team shall provide at the end of Phase 5 a final list of safety requirements applicable at building blockLevel (e.g. ETP OB, LOC OB). The latter shall then be integrated in the [OCORA-7976 - Hazard Log](#) and traced with the OCORA hazards.

Each building block defined in the Capella model on the physical architecture and analysed as safety critical shall get its own safety requirements, in accordance with [\[SUBSET-091\]](#).

At this step of the OCORA program, SRAC may have been identified for one or several requirements. To avoid creating dependencies between building blocks which could create weaknesses in the interoperability context (i.e. responsibilities are shared between two building blocks and likely two vendors), the SRAC must be re-injected into the receiving building block.

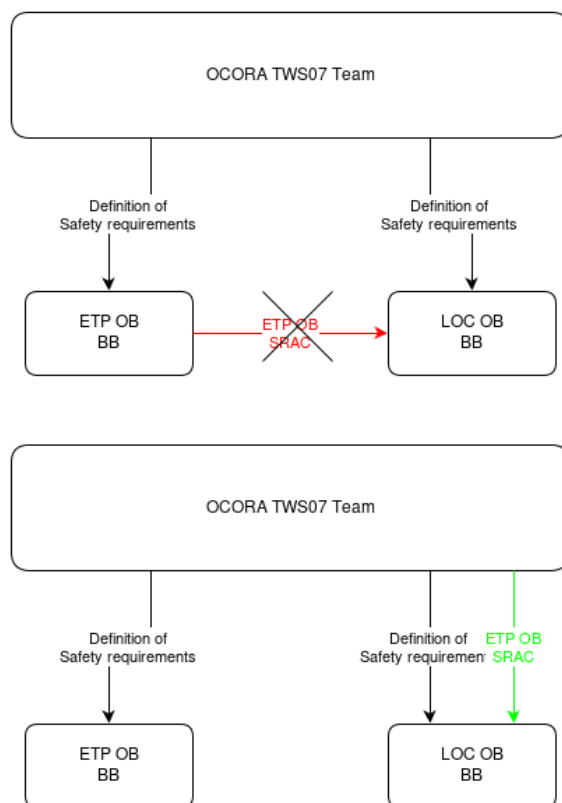


Figure 15 SRAC emission strategy

Thanks to this, no interdependence are created between the two building blocks safety cases; they are fully independent. This is possible as the OCORA program is built as a "top down" system definition and therefore, masters the overall architecture of the CCS OB.

However, to ensure that this kind of translation of safety requirements is possible, the following rules shall be respected:

- Each System function identified in the System Analysis Capel model shall be allocated to a single building block.
This also concern the TFFR allocation.
- Each Safety requirement shall be allocated to a single building block.

In case of conflict in the System Analysis or Logical-Physical Architecture, a refinement shall be performed to split in two the function or safety requirement to reach independence.

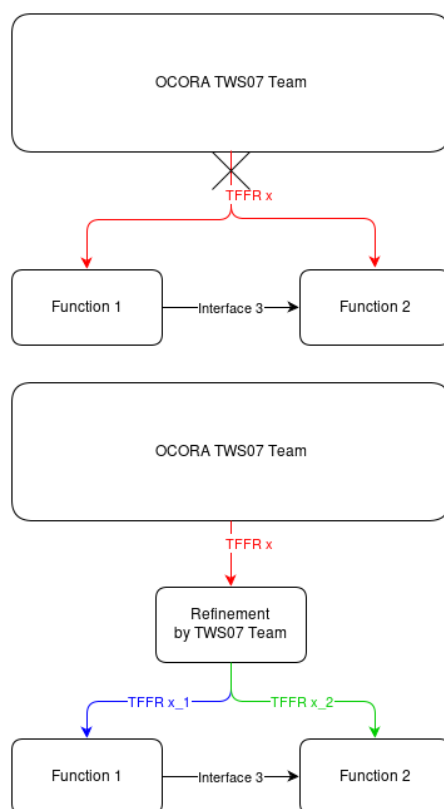


Figure 16 Refinement of safety requirements

The OCORA safety requirements shall respect the rules defined in [\[OCORA-TWS05-010\] – Requirements – Management Guideline](#).

The OCORA safety requirements shall be integrated into the OCORA set of requirements for the call for tenders (i.e. final OCORA program deliveries).

4.7.2.1.4 Design Safety Case

The OCORA TWS07 team shall terminate its activity with providing a Design Safety Case for each SuC (e.g. ETP OB BB, CCS OB). Its aim is to present a summary of the first 5 phases of the EN 50126 V cycle and show the safety case architecture of all integrated levels. This is introduced in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) and will be consolidated in a future release of OCORA.

4.7.2.1.5 Independent Safety Assessment

The OCORA initiative may require an additional opinion from an ISA when the level of requirements and processes is judged as mature enough. The scope of this activity would be to ensure the quality and safety level of all OCORA requirements for call for tenders are as much as possible free from systematic failures.

This activity may be merged into a single report covering phase 1 to 5 (see [OCORA-10234 - Independent Safety Assessment](#)).

This is not planned up to OCORA R4.

4.7.2.2 Building Blocks suppliers

Each BB supplier shall provide all deliverables expected for EN 50126 Phase 5 and be conform to OCORA set of requirements for this building block (i.e. compliance to the requirements for the call for tenders). This phase will provide crucial requirements in particular to the Building Blocks Suppliers (refer to [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) for details) who will be responsible to provide safety and interoperability conformity for their building blocks.

These requirements will be defined in future release of OCORA and later in the project development. It must be noticed that Phase 5 is voluntary shown as split between OCORA and the building block suppliers in [OCORA-7943 - Safety Planning](#). This is because OCORA ends at the granularity of the building blocks (i.e. block box). Then, each building block supplier is responsible for creating its own building block architecture (i.e. white box) with integration for instance of one or several hardware boards, redundant processors or multi-core split...

4.7.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) provide all deliverables expected for EN 50126 Phase 5 and be conform to OCORA set of requirements for this integration level.

These requirements will be defined in future release of OCORA and later in the project development.

4.7.2.4 Railway Undertakings

Each RU shall provide all deliverables expected for EN 50126 Phase 5 and be conform to OCORA set of requirements for the system level.

These requirements will be defined in future release of OCORA and later in the project development.

4.8 Phase 6 "Design and implementation"

4.8.1 Objective

Phase 6 aims at realizing the different Building Blocks by different suppliers based on the set of requirements provided by the OCORA initiative in phase 5. The goal, when phase 6 is over is to deploy the design documentation into the supplier's manufacturing facilities to produce the building Blocks.

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

The objectives of this life cycle phase are to:

- a) create subsystems and components conforming to RAMS requirements;*
- b) demonstrate subsystems and components conform to RAMS requirements;*
- c) refine plans for future life cycle tasks involving RAMS.*

4.8.2 Activities and responsibilities

4.8.2.1 OCORA initiative

The OCORA initiative has no specific activity to perform during phase 6.

The OCORA initiative shall continue to support the different stakeholders related to OCORA requirements implementation and be reactive in case of change requests are raised by the users.

4.8.2.2 Building Blocks suppliers

At this step, the suppliers shall fully design their components (e.g. hardware, software, mechanical) and written all user's documentation (e.g. installation, operational, maintenance manuals) according to OCORA requirements for call for tenders.

The supplier shall also have a manufacturing process mature to be deployed in the next phase.

(if relevant) The supplier shall share with its original RU/ integrator customer the scope of proprietary SRAC/AC for the Building Block(s) for approval (to be started in Phase 5 for the potential proprietary ones) as defined in [\[OCORA-TWS07-030\] - RAMS SRAC-AC Management](#).

4.8.2.3 Integrators

No activity is expected here from the integrator as it is not designing any element.

4.8.2.4 Railway Undertakings

(if relevant) The RU shall review and come to an agreement with the proposed set of SRAC/RAC emitted by the BB supplier. This can be started in Phase 5 for the potential proprietary ones as defined in [\[OCORA-TWS07-030\] - RAMS SRAC-AC Management](#).

4.9 Phase 7 "Manufacture"

4.9.1 Objective

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

The objectives of this life cycle phase are to:

- a) manufacture the subsystems and components;*
- b) establish and apply RAMS-centred assurance arrangements.*

4.9.2 Activities

4.9.2.1 OCORA initiative

The OCORA initiative has no specific activity to perform during phase 7.

The OCORA initiative shall continue to support the different stakeholders related to OCORA requirements implementation and be reactive in case of change requests are raised by the users.

4.9.2.2 Building Blocks suppliers

Building block suppliers are responsible to manufacture their building blocks.

4.9.2.3 Integrators

No activity is expected here from the integrator as he/she is not manufacturing any element.

4.9.2.4 Railway Undertakings

No activity is expected here from the RU as it is not manufacturing any element.

4.10 Phase 8 "Integration"

4.10.1 Objective

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

The objectives of this life cycle phase are to:

- a) assemble and install the integrated system, total combination of subsystems and components required to form the complete system;
- b) demonstrate that integrated system, subsystems and components work together as defined by the interfaces;
- c) demonstrate that integrated system, subsystems and components meet their RAMS requirements;
- d) initiate system support arrangements.

4.10.2 Activities

4.10.2.1 OCORA initiative

The OCORA initiative shall define a relevant strategy to perform a "safe integration" as stated into [\[ERA 1209-063\] Clarification note on safe integration](#) adapted to the specific OCORA compliant systems. This has been introduced into [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) with a focus on the assessment and authorization aspects and will be completed in a future release of OCORA.

4.10.2.2 Building Blocks suppliers

The building block supplier shall provide support to the different integrators when building the CCS OB system. This is introduced in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) and will be completed in a future release of OCORA.

4.10.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) shall provide all deliverables expected for EN 50126 Phase 8.

The integrators shall perform the safe integration according to [\[ERA 1209-063\] Clarification note on safe integration](#) plus the future OCORA guideline that will be defined in a future release.

4.10.2.4 Railway Undertakings

Each RU shall provide all deliverables expected for EN 50126 Phase 8 and be conform to OCORA set of requirements for the system level.

These requirements will be defined in future release of OCORA and later in the project development.

4.11 Phase 9 "System Validation"

4.11.1 Objective

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

The objectives of this life cycle phase are to:

- a) confirm by examination and provision of objective evidence that the system under consideration in combination with its Safety-Related Application Conditions complies with the RAMS requirements;
- b) confirm or update the safety case for the system under consideration, according to the results of the validation.

4.11.2 Activities

4.11.2.1 OCORA initiative

The OCORA initiative provides an overall strategy for building the whole approval process from building blocks to the final Authorisation for Placing On the Market (APOM) as required in [\[Directive 2018/545\]](#).

The later is available in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#).

4.11.2.2 Building Blocks suppliers

The building block suppliers shall provide to the integrators all approval documentation required to realise the full optimized approval process according to [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#).

4.11.2.3 Integrators

The integrators shall provide to the RU all approval documentation required to realise the full optimized approval process according to [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#).

4.11.2.4 Railway Undertakings

The RU is responsible to create all files, including SASC, to prepare the final homologation steps in phase 10.

4.12 Phase 10 "System acceptance"

4.12.1 Objective

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

The objectives of this life cycle phase are to:

- a) assess compliance of the total combination of subsystems, components, their interfaces and Safety-Related Application Conditions with the overall RAMS requirements;*
- b) accept the system for entry into service.*

4.12.2 Activities

4.12.2.1 OCORA initiative

The OCORA initiative shall provide means to ensure that all SRAC (if any) have been correctly implemented and covered in the phases 8 and 9. This is defined in [\[OCORA-TWS07-030\] - RAMS SRAC-AC Management](#). This document will be updated and completed in a future release of OCORA.

4.12.2.2 Building Blocks suppliers

The building block suppliers shall provide support to the integrators and/or the RU for safety covering the building block SRACs.

4.12.2.3 Integrators

The integrators shall provide support to the RU for safety covering intermediate systems' SRACs.

4.12.2.4 Railway Undertakings

The RU is responsible to request the APOM according to [\[Directive 2018/545\]](#) and eventually additional homologation for the concerned NSA (out of OCORA program scope).

4.13 Phase 11 “Operation, maintenance and performance monitoring”

4.13.1 Objective

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

The objective of this life cycle phase is to operate, maintain and support the system under consideration such that compliance with RAMS requirements is maintained. This includes continuously monitoring and evaluating the RAMS performance of the system and deriving measures to address shortcomings and to achieve improvements.

4.13.2 Activities

4.13.2.1 OCORA initiative

The OCORA initiative shall provide artifacts to help at operating the building blocks (and the systems where they are integrated) to reach the [\[OCORA-BWS03-020\] - Guiding Principles](#).

The OCORA TWS07 team will provide artifacts to (not exhaustive):

- Perform CBM, at BB and CCS OB levels (to be developed in a future release of OCORA),
- Perform safe and non-safe evolutions from building block to top level System level in a more flexible way, (refer to [\[OCORA-TWS07-020\] - RAMS Evolution management](#)),
- Ease cross-acceptance when integrating building block previously assessed in other contexts ([\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#),

4.13.2.2 Building Blocks suppliers

The building block suppliers shall follow the list of artifacts provided by the OCORA Initiative for phase 11 to decrease the LCC of their building blocks.

These artifacts will be completed a in future release of OCORA.

4.13.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\] - RAMS Optimized Approval Process](#) shall follow the list of artifacts provided by the OCORA Initiative for phase 11 to decrease the LCC of their integrated systems.

These artifacts will be completed a in future release of OCORA.

4.13.2.4 Railway Undertakings

Each RU shall follow the list of artifacts provided by the OCORA Initiative for phase 11 to decrease the LCC of their integrated systems. In addition, each RU shall perform its operational and hazard safety analysis. This analysis is performed using a HAZOP method (carried out with participation of all the necessary experts and users, particularly RU's and maintainers, application engineers, ...). It aims at identifying the hazards related to the installation, operation (including degraded modes) and maintenance phases of the system lifecycle (phases following design and implementation, where effects of human errors is dominant in terms of risk over components failures).

These artifacts will be completed a in future release of OCORA.

4.14 Phase 12 “Decommissioning”

4.14.1 Objective

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

The objective of this life cycle phase is to control RAMS implications of system decommissioning and disposal tasks.

4.14.2 Activities

4.14.2.1 OCORA initiative

This phase is left to the responsibility of each stakeholder involved in OCORA compliant systems. There are no specific requirement coming from the OCORA Initiative related to decommissioning.

4.14.2.2 Building Blocks suppliers

Each building block supplier shall provide all deliverables expected for EN 50126 Phase 12.

4.14.2.3 Integrators

Each integrator identified in [\[OCORA-TWS07-040\]](#) - RAMS Optimized Approval Process shall provide all deliverables expected for EN 50126 Phase 12.

4.14.2.4 Railway Undertakings

Each RU shall provide all deliverables expected for EN 50126 Phase 12.

5 RAM Activities

5.1 Objectives

5.1.1 RAM

This chapter describes the objectives, approach, specific activities and deliverables related to Reliability, Availability and Maintainability (RAM) for the first (5) phases of the EN-50126-2. The information in this document is based on and fully compliant with the RAM Strategy [OCORA-TWS07-050].

This document contains:

- the specific activities required within each phase to achieve the desired objectives
- the applicable boundary conditions for RAM
- the deliverables at the end of each phase
- the organization which is responsible and accountable for the activities
- the assurance of the required quality of the deliverables
- the planning for the required activities and milestones

Secondly, this chapter contains some background information on RAM methodologies and parameters which are important for interpretation of the RAM deliverables of the plan.

5.1.2 Life Cycle Cost (LCC)

According to the RAM Strategy [OCORA-TWS07-050], the overarching objectives for Life Cycle Costs (LCC) are to:

- lower the Life Cycle Costs as much as possible, to prevent that design changes must be made during the operational phase,
- to include activities in the RAM Plan to estimate the Life Cycle Costs of the open onboard CCS.

5.2 Approach

5.2.1 Introduction

In this section the specific objectives, approach, activities for RAM are described for each of the of the first (5) phases of EN-50126-2 [7], which are:

- Phase 1 “Concept”,
- Phase 2 “System Definition and Operational Context”,
- Phase 3 “Risk Analysis and Evaluation”,
- Phase 4 “Specification of System Requirements”, and
- Phase 5 “Architecture and apportionment of system requirements”

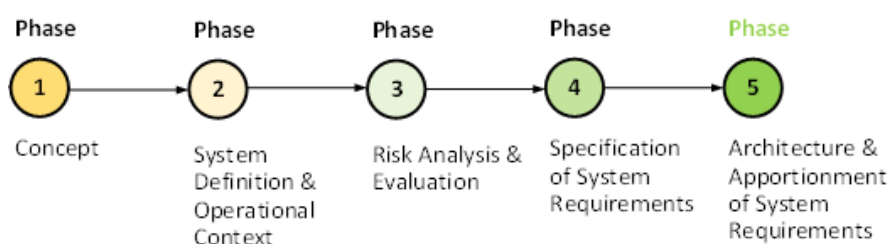


Figure 17: Phases from EN 50126-1 covered in the RAM Plan

According to the EN 50126-1:

1. the Reliability activities shall include:

- reliability analysis and prediction,
- reliability planning,
- reliability testing, and
- reliability data acquisition and assessment.

2. the Availability activities shall include:

- availability analysis,
- sensitivity analysis, and
- availability data acquisition and assessment.

3. the Maintainability activities shall include:

- maintainability analysis and prediction,
- maintainability planning, and
- logistic support evaluation.

5.3 Phase 1 “Concept”

5.3.1 Objective

The objective of Phase 1 “Concept” is to develop a sufficient understanding of the system to ensure a proper performance of all subsequent RAMS life cycle activities by identifying the environment of OCORA CCS system and creating a RAM Strategy.

The operating conditions and the mission profile for OCORA CCS has to be known and shall be respected in the design process. This affects principally:

- Environmental conditions (temperature, humidity, altitude)
- Maintenance strategy
- Operating hours of the vehicles

5.3.2 Activities

RAM activities	Responsible
Define a RAM Strategy	RAM Team
Prepare a template for collecting the RAM Data	RAM Team
Consider RAM Implications of Project	RAM Team
Define a QPRAMSS Strategy	RAM Team

5.3.3 Phase 2 “System Definition and Operational Context”

5.3.4 Objective

The objective of Phase 2 “System Definition and Operational Context” is to:

- define the OCORA CCS system (incl. the boundaries) and its mission profile (see previous chapters);
- establish the initial RAM plan for the system (this document);
- define the organisation for RAM management of the system
- Perform Preliminary RAM Analysis
- Identify Influence on RAM of Existing Constraints

5.3.5 Activities

RAM activities	Responsible
Prepare the RAM Plan (this document)	RAM Team
Collection and analysis of the RAM Data coming from the field	RAM Team
Coordination with Quality, Safety and Security responsible persons for ensuring the application of the QPRAMSS Strategy	RAM Team
Identify the reliability relevant functions at a OCORA CCS and their impact on the vehicle reliability.	RAM Team
Identify reliability relevant functional interfaces between the OCORA CCS system.	RAM Team

5.4 Phase 3 “Risk Analysis and Evaluation”

5.4.1 Objective

No specific RAM objectives are foreseen by the 50126 in Phase 3 “Risk Analysis and Evaluation”.

5.4.2 Activities

RAM activities	Responsible
Perform a FMEA as basis for building a Fault Tree Analysis	RAM Team
Establish a reliability FTA for calculating the reliability parameters	RAM Team

5.5 Phase 4 “Specification of System Requirements”

5.5.1 Objective

The objective of Phase 4 “Specification of System Requirements” are to:

- specify the overall RAM requirements for the system under consideration;
- specify the overall demonstration process and criteria for acceptance of RAM of the system;
- provide a comprehensive and identified set of requirements for the subsequent life cycle phases;
- specify necessary monitoring requirements according to the process for analysing operation and maintenance performance arranged in the Safety Plan

5.5.2 Activities

RAM activities	Responsible
Define realistic operating conditions and operating instructions to be used for operational reliability (used for calculation and tests)	RAM Team
Define the reliability and maintainability requirements	RAM Team
Define the RAM acceptance criteria	RAM Team
Allocate to each reliability relevant function reliability design target figures	RAM Team
Prepare the RAM Requirements Specification	RAM Team
Update of the RAM Plan and of all performed RAM Analyses	RAM Team

5.6 Phase 5 “Architecture and apportionment of system requirements

5.6.1 Objective

The objective of Phase 5 “Architecture and appointment of system requirements phase are to:

- apportion the RAM requirements to the designated subsystems and/or components;
- describe the RAM requirements and specify the interfaces for all subsystems and components
- define the acceptance criteria to demonstrate fulfilment of the RAM requirements for the system, subsystem, equipment in subsequent lifecycle phases;


5.6.2 Activities

RAM activities	Responsible
Apportion the reliability design target figures across the OCORA CCS stakeholders to ensure that the integration allows to meet the OCORA CCS reliability requirements.	RAM Team
Update and consolidate of the RAM Plan and of all performed RAM Analyses	RAM Team

6 Cyber-security Activities

The activities performed in by the cyber-security team are defined in [\[OCORA-TWS06-010\] - \(Cyber\) Security - Project Security Management Plan](#).

7 Synchronisation activities

The strategy for synchronisation activities is presented into the  [RAMSS Policy](#).

8 Decisions and issues

8.1 Decisions

OCORA-10204 - System Definition to create

Because of the transition period between OCORA and ERJU, the creation of System Definition is for now on hold. It will be reevaluated in the workstream definition of R5.

8.2 Issues

OCORA-10171 - No more Testing activities in OCORA

From R4, the TWS09 - Testing group is no more active. Therefore, all activities related to testing are on hold. It implies that no test cases can be created to validate OCORA requirements until a solution is defined.

OCORA-10172 - No quality team for OCORA

Up to R4, there is no WS assigned to hold this role up to now. Therefore, the activities are split between TWS07 and the CORE Team of OCORA.

OCORA-10173 - No more cyber-security team in OCORA

From R4, the TWS06 - Cyber-security group is no more active. Therefore, all activities related to cyber-security are on hold.

OCORA-10238 - No overall functional breakdown available

Up to R4, no overall functional model of the system is available. This means that the TWS07 team cannot close Phase 2 and move on Phase 3 until the latter is available.

9 Annex - QRAMSS deliverables

To be filled in a future release of OCORA.