OCORA

Open CCS-OB Reference Architecture

RAMS – Modular Safety Strategy

Document ID: OCORA-TWS07-010

Version: 3.51

Date: 24.11.2023

Revision history

Version	Change Description	Initial	Date of change
1.03	Official version for OCORA Delta Release	JB	30.06.2021
1.90	Update for R1	MM	26.11.2021
2.00	Update following Rolf M. comments	JB	02.12.2021
2.10	Update for R2	PN	30.05.2022
2.20	Official version for OCORA Release R2	PN/JB	09.06.2022
3.00	First draft for R3	JB	29.06.2022
3.10	Update before TWS07 review	JS	10.11.2022
3.20	Update following TWS07 comments	JB	18.11.2022
3.30	Final update for R3	JB	01.12.2022
3.40	Review for R4	VI	12.06.2023
3.50	Update for R4	JB	26.06.2023
3.51	This document served as input for the ERJU System Pillar PRAMS domain and will be continued there. It remains published for information purposes only.	MM	24.11.2023

Table of contents

Table of figures

References

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

The following references are used in this document:

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-040 – Feedback Form

[3] OCORA-BWS01-020 – Glossary

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

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

[6] OCORA-BWS04-010 – Problem Statements

[7] OCORA-BWS06-010 – Economic Model – Introduction & Overview

[8] OCORA-BWS09-010 – Acceptance of Global Standards

[9] OCORA-TWS01-010 – System Requirements

[10] OCORA-TWS01-030 – System Architecture

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

[12] OCORA-TWS05-020 – Stakeholder Requirements

[13] OCORA-TWS07-020 – Evolution Management

[14] OCORA-TWS07-030 – SRAC/AC Management

[15] OCORA-TWS07-040 – Optimized Approval Process

[16] OCORA-TWS07-050 – RAM Strategy

[17] OCORA-TWS07-100 – CENELEC Phase 1 – Concept

[18] OCORA-TWS07-060 – Configuration Management – Concept

[19] OCORA-TWS09-010 - Testing Strategy

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

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

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

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

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

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

[26] EN 50506-1: 2007 - Railway applications — Communication, signalling and processing systems — Application Guide for EN 50129 — Part 1: Cross-acceptance

[27] TS 50701:2021 - Railway applications - Cybersecurity

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

[29] SUBSET-088 part 3: ETCS Application Levels 1 & 2 - Safety Analysis - Part 3 - THR Apportionment

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

[31] TSI LOC&PAS: COMMISSION REGULATION (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union

[32] TSI CCS Application Guide GUI/CCS TSI/2019

[33] CSM-RA 402/2013 – Common Safety Method for Risk evaluation and Assessment

[34] ERA 1209-063 Clarification note on safe integration

[35] List of CCS Class B systems - ERA/TD/2011-11 V 4.0

[36] REGULATION (EU) 2018/545 - vehicle authorisation and railway vehicle type authorisation process

[37] DIRECTIVE (EU) 2016/797 - on the interoperability of the rail system within the European Union

[38] DECISION 2010/713/E - on modules for the procedures for assessment of conformity, suitability for use and EC verification to be used in the technical specifications for interoperability

[39] ED Decision 2018/008/R Annex IV AMC 20-170, "Integrated modular avionics (IMA)"

1 Introduction

1.1 Purpose of the document

This document is addressed to safety managers that are involved into the realization of OCORA compliant ETCS or CCS-OB systems (ETCS-OB, CCS-OB) acting as contracting entities, builders, integrators, manufacturers, and assessors.

It is also addressed to experts in the CCS domain and to any other person, interested in the OCORA technical concepts for on-board CCS. The reader will gain insights regarding the topics listed in chapter 1.1 and is invited to provide feedback to the OCORA Collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA release documentation can be given by using the feedback form [2].

This document aims to provide the reader a roadmap regarding the different steps required to deploy safety activities within a new modular architecture of a CCS-OB system (CCS-OB) as defined in TSI CCS [20]. A focus is done on the following topics:

- Introduction to Modular Safety (chapter 2)
- OCORA stakeholders (chapter 3)
- OCORA RAMS documentation (chapter 4)
- Modular Safety Strategy (chapter 5)
- Safety Case Management (chapter 6)

The Modular Safety Strategy is evolving in parallel with other OCORA Workstreams (e.g. Architecture, Testing, FVA, Cybersecurity etc.) which iteratively integrate the consequences of the Modular Safety Strategy. So there will be OCORA Collaboration requirements in other workstreams and the Modular Safety Strategy will incorporate them once they are finalized.

OCORA Collaboration (or sometimes also called OCORA Project) represents the activities performed by the OCORA members coming from SNCF, SBB, ÖBB, DB and NS to realise the official set of documents that will be finally used by the industry and railway operators for the call for tenders for new CCS-OB systems. A more detailed presentation is provided in the OCORA Concept [17]. The present document has been realised by the RAMS team, identified as TWS07 within OCORA Collaboration. This team involves safety managers from the companies involved in OCORA with different skills and background to benefit of a large scope of return of experience.

1.2 Applicability of the document

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

1.3 Context of the document

This document is published as part of an OCORA release, together with the documents listed in the Release Notes [1]. It is the second release of the Modular Safety Strategy, and it is still in a preliminary state. Before reading this document, it is recommended to read the Release Notes [1], the Introduction to OCORA [5], the Problem Statements [6] and the Set of Requirements [9]. The reader should also be aware of the Glossary [3] where all the used acronyms in these documents are issued. The Modular Safety whitepaper issued in OCORA release R1 has been used as basis to publish this modular safety strategy. Thus, it will not be updated anymore and only the present document remains the reference for OCORA modular safety.

2 Introduction to Modular Safety Strategy

This section aims at defining what is commonly called “Modular Safety” in the context of OCORA. The present document describes “Modular Safety” in deeper details and presents a complete overview of it.

2.1 Why Modular Safety?

Safety is a mandatory requirement for CCS solutions. The current standards use a monolithic approach for CCS-OB systems (CCS-OB). This is reflected in the absence of clear borders between the individual modules of the CCS system, causing many proprietary interfaces and dependencies. Suppliers of individual modules define their own system boundaries. This results in a wide spread of safety related application conditions (SRAC) throughout the CCS system. Dealing with these SRAC increases the complexity of the system which can result in safety issues caused by misunderstandings at different integration levels.

Because of the monolithic approach, changes to individual modules are impossible without impacting the complete system. This limits the evolution of the CCS-OB system because a lot of reassessment work is needed when upgrading the system. The impact is usually so expensive that the non-mandatory evolutions are withdrawn and thus, the CCS-OB system does not evolve as it is expected over its lifetime. This makes the economic viability of the CCS-OB system low.

A modular safety approach will allow a much easier evolution of the CCS-OB system than today. The upgradeability and interchangeability of the individual modules will be increased. This allows changes to be implemented cheaper and quicker. The modular approach (i.e. with standardised interfaces) will also avoid vendor lock-in caused by the intertwining of the CCS-OB modules. This avoidance makes railway undertakings more flexible regarding suppliers’ choice.

Without mastering modular safety, these goals cannot be reached. Modular safety is therefore a clear enabler for OCORA.

2.2 What refers to Modular Safety?

2.2.1 What is Modular Safety and its Purpose

The RAMS workstream within OCORA Collaboration will provide a set of documents (e.g. optimised processes, requirements) by which the safety activities related to the OCORA compliant programs shall be conducted.

Modular Safety shall:

- take advantage from and support the modular architecture of the OCORA initiative: safety activities are based on an architecture made by modular building blocks with standardised interfaces;
- support new and retrofit projects by providing a harmonised strategy for integrating the required building blocks composing a CCS-OB system as well as the interaction between the OCORA compliant systems and the rolling stock equipment (e.g. emergency brakes, TCMS) through a train adapter. The latter is identified in [11] and introduced in section 6.1.2.;
- support a harmonised strategy to allow a fluent deployment of evolutions (e.g. upgrades, new functionalities) of the OCORA CCS-OB system and its constituents, reducing the certification efforts at all levels (initial- and re-certification) without degrading safety;
- define the safety elements necessary to allow the homologation of the OCORA stand-alone building blocks and the integrated CCS-OB system.

2.2.2 Modular Safety goals

Considering as a given the OCORA target system, the Modular Safety requirements set will be developed to fulfil the following goals:

- clear definition of roles, tasks and responsibilities of the different stakeholders, thanks to the defined target scenarios;
- definition of safety requirements and targets (e.g. hazardous events, TFFR) for the building blocks and their interfaces to be ordered as standalone sub-systems (i.e. with their own ISA, NoBo, DeBo, AsBo certificates);
- simple and standardised safe and non-safe application conditions (AC/SRAC) for the building blocks, thanks to a robust interface design;
- clear and comprehensive safety concept of the “black box” behaviour, thanks to the modular target system design;
- broad acceptance of assessors/assessment methods, thanks to a clear cross-acceptance methodology;
- standardisation of impact analyses and the assessment panel, thanks to a dedicated methodology for evolution management which will result in a reduction of cost and time for end-to-end evolution management (i.e. from change to assessment);
- prevent the “Domino-effect” of re-assessment and tests when updating the part of the CCS as it is now necessary to re-assess and re-test all the inter-dependant software and hardware.

2.3 Barriers for Modular Safety implementation

What is hindering modular safety to be implemented and why it is not already implemented?

Vehicle suppliers act in most cases as integrators of different subsystems from different suppliers. Integrators usually manage safety and allocate safety requirements already in early stages of the life cycle (see EN 50126-1 [21]) towards their suppliers. Motivation for that is based in the very same area as the OCORA objectives: enable evolution, enable inter/exchangeability, manage obsolescence and promote competition (refer to [6] and [7] for more details).

There are other barriers, but they are typical for any change process.

- Systems/subsystems/components might not be on the market yet. This means that the unavailability of the OCORA CCS-OB constituents at the call for tender’s time could lead the contracting entity to cancel his wish to migrate to an OCORA compliant system for a solution already deployable in a shorter period (i.e. legacy monolithic approach).
- Existing specifications might be too strict or too open regarding architecture or might show gaps in requirements.
- The first integrator or manufacturer to follow the modular safety approach might run into the typical quality / cost / delay dilemma. Indeed, the reuse and distributed engineering, which results in too complex solutions, become hard to be understood in terms of safety (e.g. safety managers and assessors).

3 OCORA's stakeholders and environment

3.1 Legal and regulative context

Prior to presenting the safety case nesting, clarification shall be brought about the different stakeholders that will be involved in OCORA compliant projects/programs.

The need to define this list at the very beginning of an OCORA compliant program/project comes from the return of experience from the IMA (Integrated Modular Avionics [39]) where modular systems are deployed for several years now. Indeed, the avionics return of experience shows that when deploying a modular architecture, each stakeholder shall be clearly defined with precise tasks and responsibilities. Furthermore, all these independent stakeholders must be managed and coordinated by an overall stakeholder that ensures smooth communication, integration and safety data workflow between them.

In a parallel development, ERA has realised its own return of experience on the vehicle authorisation process [36] because the concept of "safe integration" defined in the latter was misunderstood (i.e. a limited scope of activities was deployed by the directive's applicants).

Thus, ERA has emitted a document called ERA 1209-063 Clarification note on safe integration [34] where information is proposed to handle the "safe integration" in a generic way and also when dealing with vehicle authorisations.

> *The EU railway stakeholders have different understandings of the concept of "safe integration". Safe integration is often and wrongly understood only as the demonstration of the technical compatibility and of the correct technical interfacing between sub-systems [e.g. check of technical compatibility between the vehicle and the network(s)]. In practice, safe integration is an inherent part of a systematic risk assessment and risk management process (1), also within every structural sub-system. The concept of "safe integration" has thus a broader meaning and goes beyond the single check of the technical compatibility, or correct technical interfacing, between several sub-systems brought together. Safe integration applies also at different levels and to the entire life cycle of the design, operation, maintenance, and disposal/decommissioning of the railway system and of its components.*

The idea for OCORA is to get inspiration from these two sets of information (i.e. IMA [39] and ERA [34] note) to propose a generic and common list of roles that shall be assigned at the beginning of any new OCORA compliant program/project to fulfil the "safe integration" expectations from ERA when deploying a modular safety architecture.

Modular safety strategy introduces these roles and their relationship related to safety activities. However, the overall definition of each actor with its role, tasks and responsibilities is presented in the OCORA Glossary [3].

Figure 1 presents the list of all railway actors for vehicles and network from a high-level point of view (i.e. vehicle authorisation). Only a part of them is directly involved inside OCORA compliant projects/programs. Thus, the latter has been used as input to realize a focus diagram showing only the key actors having a direct impact on modular safety and the safety workflow between them. This is presented in **Figure 2**.

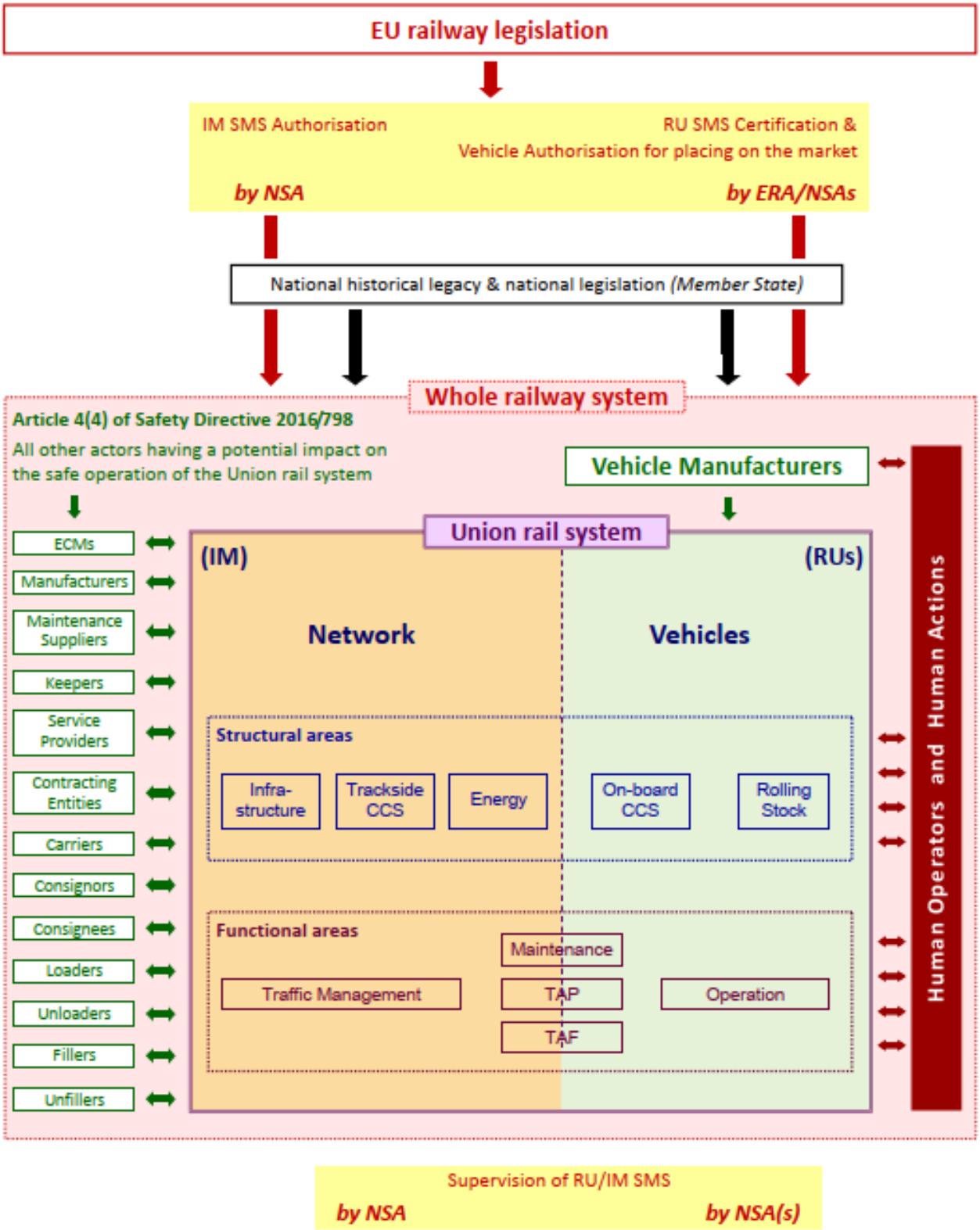


Figure 1 ERA list of railway stakeholders (from [34])

When dealing with a modular architecture, new roles come up which are not clearly defined in the conventional approach. This is the case for:

- *CCS-OB Builder;*
- *Vehicle Preparator;*
- *CCS-OB integrator.*

Indeed, today, the *CCS-OB Builder* is always the CCS-OB supplier because current systems are provided as monolithic blocks, composed of proprietary elements and proprietary internal interfaces.

In addition, the *CCS-OB integrator* and the *Vehicle Preparator* used to be the rolling stock supplier and most of the time they came from the same company.

A modular architecture points out that these two roles can now be handled by third party(s), chosen by the *contracting entity*. OCORA defines for them clear tasks, roles and responsibilities in the glossary [3] and any *contracting entity* shall use these definitions with the integrators to avoid possible conflicts or grey areas where the responsibilities and activities are not allocated.

When dealing with an OCORA modular architecture, the most critical role to allocate is the *CCS-OB Builder*. The latter shall coordinate the activities of the different suppliers to integrate their sub-systems and ensure that ISA and NoBo (plus DeBo and AsBo when required) certificates of the CCS-OB system will be delivered by the assessor.

The complete list of tasks and responsibilities for all stakeholders is defined into the Optimised Approval Process [15].

The different workflows regarding assessment activities as well as the SRAC/AC flows (bottom-up) are shown in **Figure 2** and described below.

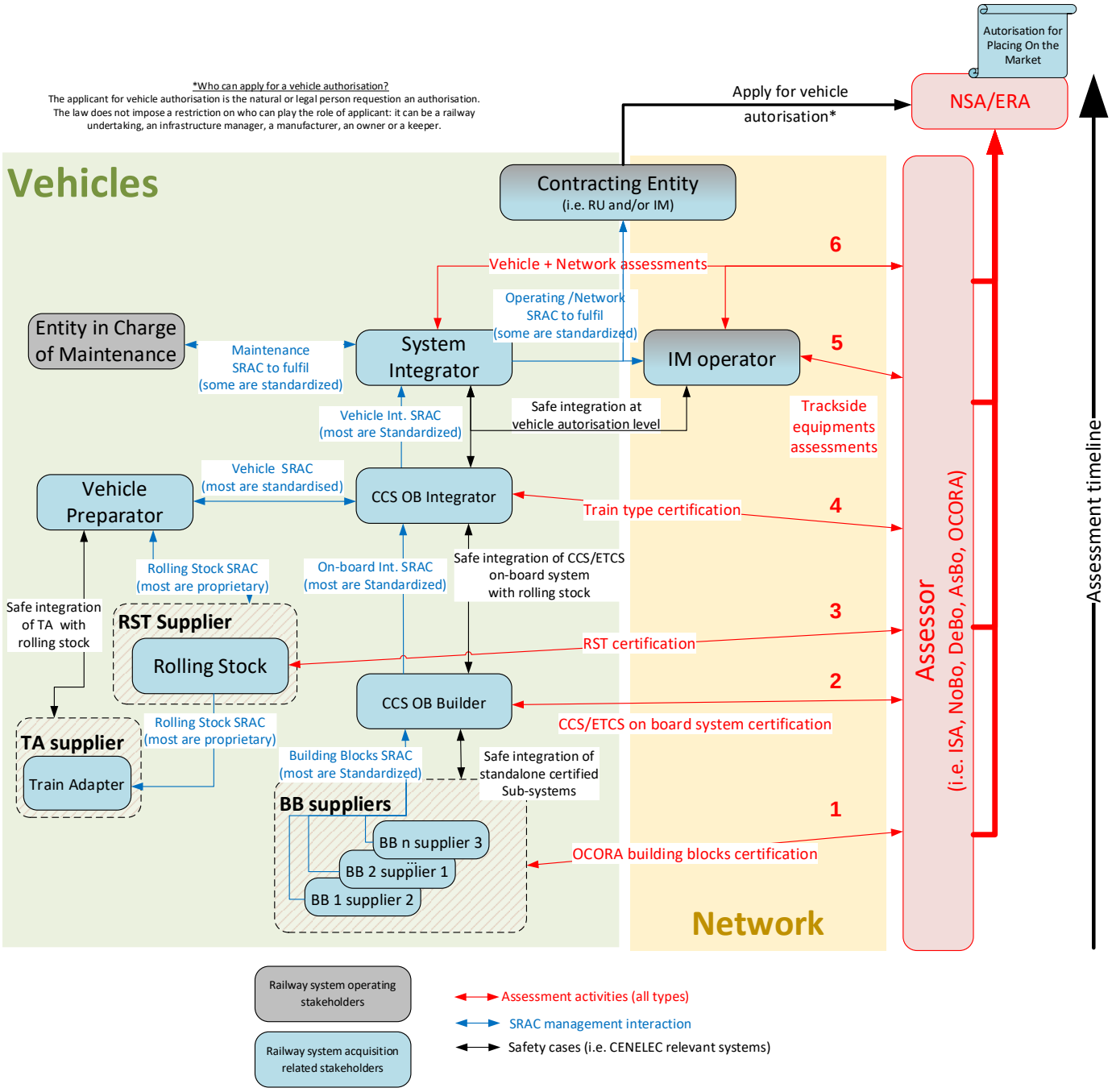


Figure 2 OCORA Modular Safety stakeholders

- **Assessment activities (written in red in Figure 2):**
  - **OCORA building blocks certification (1):** one important goal of OCORA is that a CCS-OB system can be built based on different suppliers' building blocks. The certification scope of activities is presented in section 5.4.
  - **CCS/ETCS on board system certification (2)**: this activity, led by the newly defined role in the railway world; *CCS-OB Builder*, represents the heart of any OCORA compliant system. It is also a completely new and highly critical phase of the overall vehicle homologation. Indeed, this activity requires from railway companies (e.g. manufacturers, RU operators) skills and technical background on CCS-OB systems.

    Based on a set of mandatory documents provided by OCORA Collaboration defined in the overall OCORA application guide, the *CCS-OB Builder* shall handle the assessment panel defined in Assessment activities.

- **RST certification (3)**: this activity focuses on the certification of the rolling stock (i.e. vehicle without the train adapter and the CCS-OB system). This is to be done under the responsibility of the rolling stock supplier.
- **Train type certification (4)**: this activity focuses on the integration of the CCS-OB system (i.e. scope defined by TSI CCS [28]) inside a rolling stock equipment (i.e. scope defined by TSI LOC&PAS [31]). This activity shall be realised by the newly defined *CCS-OB*. Its activities are already well defined and bordered thanks to the two TSI (i.e. [28] and [31]).

  Based on them and on the set of mandatory documents provided by OCORA Collaboration defined in the overall OCORA application guide, the integrator at train type level shall handle the assessment panel defined in Assessment activities.
- **Trackside equipments assessments (5)**: this activity represents the certification of all trackside equipments (e.g. EUROBALISES, interlocking systems, RBC) which is ensured by the suppliers and controlled by the *IM Operator*.
- **Vehicle + network assessment (6)**: this activity represents the top-level assessment where the rolling stock presents its compatibility within a dedicated network. At this level, ERA clarification note [34] and all its related mandatory regulations and standard are fully applicable to the *contracting entity*.

  OCORA Collaboration does not directly define documents for this level. However, the use of OCORA compliant systems will have a positive impact (e.g. less costs and delays) in case of evolution of one or several CCS-OB building blocks. This is presented in section 5.3.

- **Safety or non-safety-related application conditions (SRAC / AC: written in blue in Figure 2):**

  The overall management of the AC in OCORA compliant projects/programs is introduced in section 5.1.

  - **Building Block AC (most are standardised)**: this workflow represents all the different AC that a building block supplier (i.e. platform, peripheral device, application) has to emit so that its sub-system can be used in a safe way. It must be noticed that thanks to OCORA, a large part of the current proprietary internal interfaces of the CCS-OB system will be standardised. Following that, the RAMS analysis performed within OCORA Collaboration on them will result in a generic set of AC that should be harmonised and respected by all building blocks suppliers. A dedicated document (i.e. called OCORA application guideline) will manage this topic in a later phase of the OCORA program development by the OCORA RAMS team.

    Finally, only a few AC will remain suppliers dependent. They concern all non-standardised parts of the sub-system such as the internal architecture (e.g. 2oo2, 2oo3), maintenance (e.g. preventive or corrective activities) or remaining proprietary interfaces.

    It must be noted that these AC can be addressed to other building blocks or to an upper level of integration.
  - **Maintenance AC to fulfil:** this workflow presents all AC that are emitted at any level of the overall OCORA compliant project/program and provided to the *entity in charge of maintenance* by the *contracting entity*. The latter has to provide for each of them a proper coverage that will be part of the vehicle authorisation process.
  - **Operational /Network AC to fulfil:** this workflow presents all AC that are emitted at any level of the overall OCORA compliant project/program and provided to the *operators* or to the network (i.e. trackside) by the *contracting entity*. They must provide for each of them a proper coverage that will be part of the vehicle authorisation process.
  - **Rolling Stock AC to fulfil**: this workflow presents all AC that are emitted at any level of the overall OCORA compliant project/program and provided to the rolling stock supplier by the *CCS-OB Integrator*. The latter has to provide for each of them a proper coverage that will be part of the vehicle authorisation process. The rolling stock supplier can also provide AC for some building blocks and the *CCS-OB Integrator* ensures that their coverage is provided by the different involved manufacturers.

3.2 OCORA's contribution to ERJU

Europe's Rail Joint Undertaking (ERJU) is the new European partnership on rail research and innovation. The vision of ERJU is to deliver, via an integrated system approach, a high capacity, flexible, multi-modal and reliable integrated European railway network by eliminating barriers to interoperability and providing solutions for full integration, for European citizens and cargo. This partnership aims to accelerate research and development in innovative technologies and operational solutions. ERJU is based on two pillars, where the System Pillar shall deliver the system architecture on which the rail community will converge in a collaborative manner, and the Innovation Pillar supports and complements this through the underpinning concepts and detailed solution architectures, as well as proof of concepts.

ERJU is an opportunity to build and secure the OCORA trajectory as it agrees on a modularity framework and related specification and provides an open and scale constructive collaboration to progress with suppliers and as it coinvests to industrialise new commodities for rail operation. ERJU can be the short line for OCORA to be acknowledged and the OCORA MVP to be developed as a reference standard. OCORA's contribution to ERJU is summarised in the following **Table 1.**

OCORA's contribution to the System Pillar	**OCORA's contribution to the Innovation Pillar**
• PRAMSS : Performance / Reliability / Availability / Maintainability / Safety / (Cyber)Security • Modelling operation concept • Modelling CCS onboard system: from capabilities, down to logical and physical architecture • Methodology & Tooling • Testing Concept / IVV Strategy (safety/perf targets) • Interface Specifications for hardware and software building blocks	• Application prototypes for building blocks and system functionality • Test environment for certification of interoperable and interchangeable modules • Stepwise reduction of onsite testing and progressive full virtual certification • Validation/maturity reporting e.g. from prototypes or large scale demonstration

Table 1 OCORA's contribution to the System and Innovation Pillars of ERJU

4 OCORA RAMS documentation

The RAMS documentation produced by this Workstream is strongly connected to the RAMS Strategy as shown in **Figure 3**. The RAMS documentation is divided into the OCORA RAMS Strategy Whitepapers ([13], [14], [15], [16]) and the OCORA CENELEC Documentation (starting with [17]) according to EN 50126 (Phases 1-5) providing the requirements for building block development within OCORA. The RAMS Strategy can be separated in two streams: One representing the Safety Strategy, described in this paper, and one for RAM topics concerning the reliability, availability, and maintainability of OCORA conformal systems. The Safety Strategy is presented as a process flow chart with respect to the lifecycle for developing, authorising and upgrading an OCORA compliant system or building block. The colour in which the process steps are presented build the bridge to the corresponding documents within this workstream.

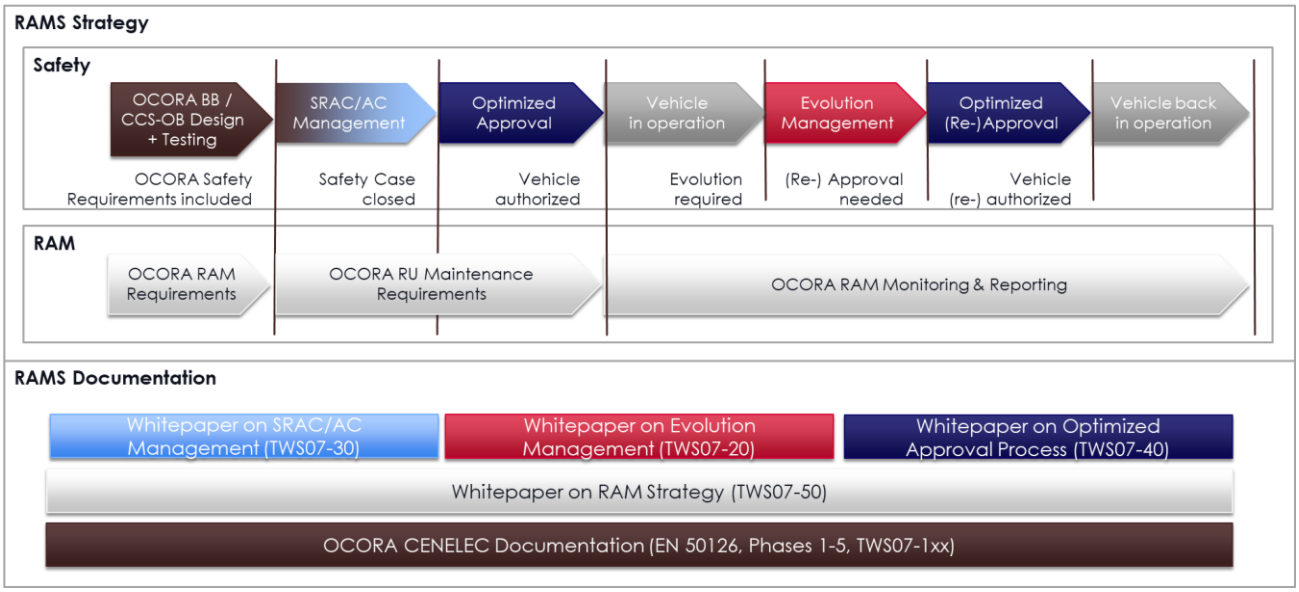


Figure 3 OCORA RAMS Strategy and RAMS Documentation

The OCORA RAMS Strategy Whitepapers which are the responsibility of the RAMS activities are provided as a "tool kit" for future projects/programs aiming at developing OCORA compliant CCS-OB systems. Some examples are identified hereafter:

- **RAMS – Modular Safety strategy (TWS07-10, present document)** to safely handle new modular CCS-OB systems deployment or the transition between a conventional CCS to an OCORA compliant one (i.e. retrofit),
- **RAMS – SRAC/AC management (TWS07-30, [14])** A methodology for handling safe and non-safe application conditions (refer to section 5.1) through OCORA compliant systems. This defines, among other topics, the rules for SRAC/AC writing and method for closing them at upper levels,
- **RAMS – Evolution management (TWS07-20, [13])** Process for safely handling evolutions (refer to section5.2) within an OCORA compliant CCS-OB system (i.e. from building block to vehicle authorisations),
- **RAMS – Optimized Approval (TWS07-40, [15])** An approval process to handle assessments (refer to section5.3) for the first OCORA compliant integrated system one and later, during its lifetime when evolutions are expected.
- **RAMS – RAM Strategy (TWS07-50, [16])** to handle RAM in a new modular CCS-OB systems deployment or the transition between a conventional CCS to a OCORA compliant one (i.e. retrofit),

The use of the set of documents delivered by the RAMS team will be part of the mandatory documentation for suppliers and integrators to finally being successfully assessed through OCORA (refer to 5.4.2).

To ensure that the OCORA deliverables presented above are developed in accordance with the CENELEC standards, the OCORA Collaboration will develop this program through a CENELEC V cycle. This is presented in the System Concept [17] (i.e. Phase 1 according to EN 50126-1 [21]).

5 Modular Safety Strategy

5.1 SRAC/AC Management

5.1.1 Context

Safety-related application conditions (SRACs) are assumptions, constraints and application rules exported from the safety case of a system under consideration (SuC) for controlling risks which cannot be mitigated within the limits of the SuC. Already recognisable from designation, the application conditions should be primary safety-relevant, therefore named as SRACs. Only if the application conditions have high impact on RAM or Cybersecurity issued, they should also be considered and just named as application conditions, ACs.

This section introduces the way to manage SRACs/ACs within OCORA compliant projects/programs. The need comes from a common return of experience from railway undertakings. Indeed, in today's railway systems, SRAC are usually a very sensitive matter to handle. The highest level of safety case uses to deal with very low level SRAC coming from the ETCS on-board manufacturer (e.g. physical system). The gap between these two levels of engineering management used to induce troubles when covering this kind of SRAC. Because of the amount of SRACs, their coverage requires a lot of time and resources in engineering, up to the final vehicle authorisation process with the assessor. Furthermore, due to the proprietary interfaces within the EVC, this coverage cannot be reused from one ETCS on-board supplier to another.

To conclude, with both the definition of complex SRAC by the downstream levels of safety cases and their quantity, the risk of wrong coverage of SRAC at the top-level project must be considered. Although rules already exist inside EN 50129 [24] for SRAC writing, their sharing between different levels of safety cases usually induces misunderstandings which can, in the worst case, drive to an incorrect coverage and lead to a safety issue. Based on discussion with OCORA members, it appeared that OCORA shall set up a guideline presenting an improved way to cover SRAC with more support from the different SRAC emitters and more strict and common rules for their definition.

OCORA provides the opportunity to improve the management of this complex subject thanks to a modular architecture. In another way, OCORA architecture needs several requirements to help at simplifying the SRAC handling. This is presented in the Whitepaper on SRAC/AC management.

5.1.2 Purpose

According to OCORA's goal to standardise the CCS-OB architecture, all the BB inside the CCS-OB should be standardised and should be connected via standardised interfaces. This is an essential precondition for simple upgrading and/or exchanging of BB. Thanks to standardised interfaces, also the safety requirements for the BB can be clearly defined and based on the overall CCS-OB hazard analysis. In addition, at a final stage, there will be no need for emitting SRACs from one BB to another or (as currently often implemented) between different levels (e.g. from one BB to the integration level within CCS-OB). In contrast to the current bottom-up approach of SRAC handling as discussed before, within OCORA's CCS-OB design, the constraints and application rules will be defined top-down from the CCS-OB system level to each standardised BB and will be handled as safety requirements.

SRACs will be only needed for interfaces outside the scope and influence of OCORA. Furthermore, in the beginning, when the first BB are realised, the situation will occur that one BB has to export some application conditions (safety-related or non-safety-related), which have not been considered by the OCORA collaboration before. For these cases, the OCORA RAMS team provides the **OCORA AC Template** as well as the **OCORA AC Management Guideline** introduced in the whitepaper on SRAC/AC management. An overview on the deliverables regarding SRAC/AC management is presented in **Figure 4**.

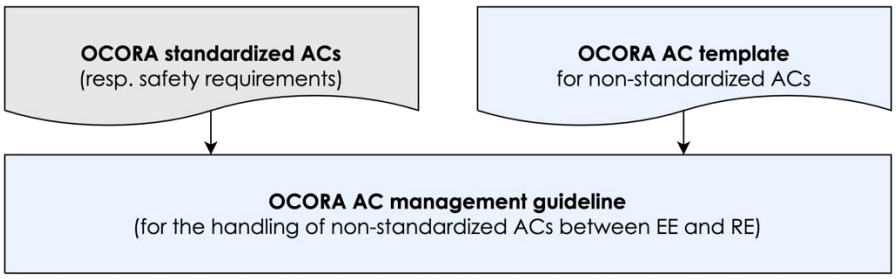


Figure 4 SRAC management deliverables of the OCORA RAMS team

The standard interfaces issued from OCORA will implicitly result in a set of **OCORA standardised ACs** at the borders of the building blocks that shall be used by any vendor or integrator dealing with OCORA in its CCS-OB system.

Unfortunately, today, it is impossible to ensure that 100% of AC at interfaces level will be standardised. Furthermore, additional proprietary AC may be emitted for topics not fully handled by OCORA (e.g. operational or maintenance scenario). This will be covered in the Whitepaper on SRAC/AC management.

5.2 Evolution Management

5.2.1 Context

Evolution management represents a large scope of activities that occur during the whole CCS-OB system lifetime. Some of them can easily be handled (e.g. modification fit, form and function of a non-safety related element) but most of them induce an impact on the certificates (e.g. ISA, NoBo) already issued (e.g. functional or interface impact). This is obviously more frequent when dealing with evolutions in a monolithic system.

For that purpose, the evolution management usually represents an important source of expenses for the operators owning monolithic on-board system. Further details can be seen in the Whitepaper [13].

5.2.2 Purpose

The evolution management of a CCS-OB system throughout its lifetime can be analysed from two different aspects: modifications due to corrective change requests (e.g. Sw bugs, non-conformities to customer's specification) or to improvements (e.g. modification of existing requirements due to un-precised initial requirement(s), new non-functional requirements, obsolescence management).

The first category represents the largest part of the CCS-OB system evolutions during the first years after its initial delivery, whereas the second one will increase all along its lifetime. **Figure 5** presents a graphical representation of the description above.

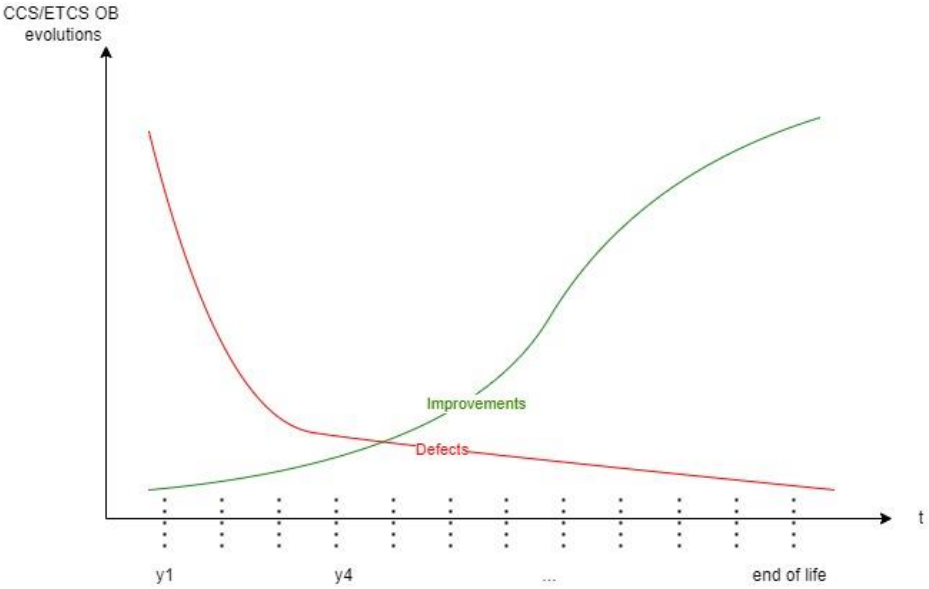


Figure 5 Evolutions during CCS OB lifetime

Regarding the impacts of these evolutions, a large part will not have a safety impact on the CCS OB system. This part is even more important regarding the “improvement” change requests. Indeed, it is obvious that unless clear failures are detected within safety mechanisms of safety related systems (e.g. voting function, Hw or Sw watchdog), the latter are rarely modified because of their complexity, criticality and cost for re-validation, re-assessment activities to be performed.

To help decreasing the impact of non-safe evolutions within OCORA, the following requirements are emitted for the future building blocks constituting OCORA compliant CCS OB systems (called “segregated systems” on **Figure 6**):

- the SuC shall be designed with non-interference rules between safe and non-safe functions;
- the SuC shall be designed with non-interference rules between cyber-secure and non- cyber-secure functions;
- the SuC shall be designed with non-interference rules between safe and cyber-secured functions.

The first part of the above requirements aims at ensuring that all change requests related to non-safe functionalities evolutions can be done without impacting the safety case of the SuC. The management of the maintainability of the current valid certificate in that context will be detailed in [13]. On **Figure 6**, this is represented by the blue arrows where no direct ISA activities are expected before putting the SuC back in commercial service. The strategy applied here is called “yearly Letter of Support”. The goals, scope and conditions of the latter are explained in the evolution management document [13].

If this is successfully implemented within each OCORA building blocks, the biggest part of the evolution management improvements is already done. This represents an important game changer for future railway equipments.

5.2.2.1 Evolution challenges for non-segregated systems

For most legacy monolithic systems built before 2010 (called “conventional systems” on **Figure 6**), no segregation between safe and non-safe functions exists. It means that anytime an evolution is required, whatever its purpose, a complete impact analysis must be done to show if the latter has a safety impact or not. In addition, any type of evolution in such systems will basically need significant verification / validation activities (e.g. regression tests) and later a recertification of the complete CCS-OB system which will, at the end lower its upgradability by realising less frequent updates from the manufacturers unless the customer is ready to pay a high cost for improvement evolutions. This is presented on **Figure 6**.

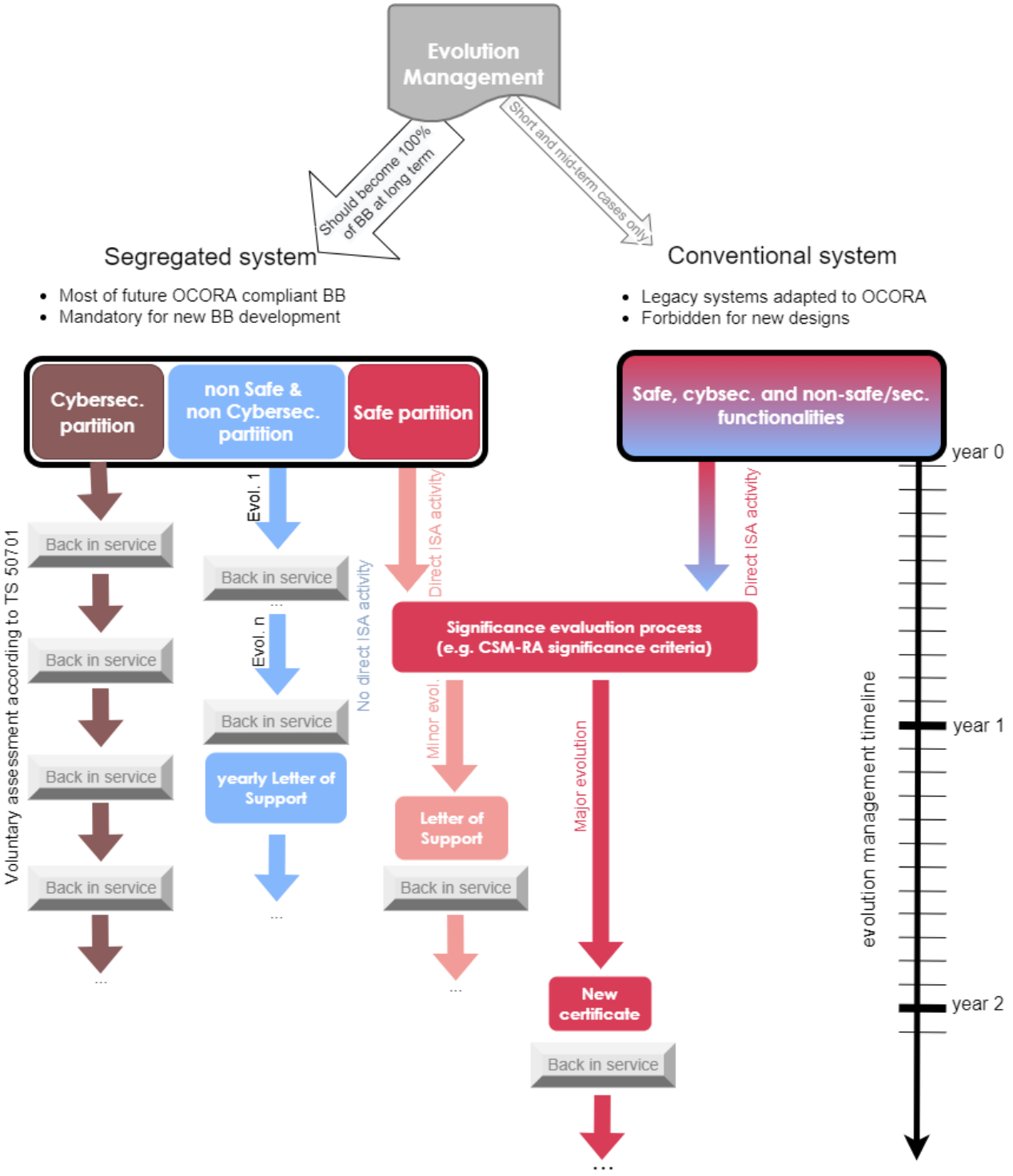


Figure 6 Goals of evolution management

5.2.2.2 Evolution challenges for segregated systems

The evolution management will also deal with the management of changes occurring on segregated safe partition and conventional safe systems with the deployment of a lighter assessment scope and activities based on a detailed impact analysis (performed by the SuC owner). This principle is based on the significance evaluation criteria used within (list not exhaustive) CSM-RA, TS 50701:2021 and EN 50128:2011 / EN50657:2017 section *9.2 – Software maintenance*. This is covered by the concept of a delta assessment called “Letter of Support” (refer to **Figure 6**) which focuses on a set of documentation created to present a dedicated set of “light” modifications beside the original technical file used for the safety case. The detailed goals, scope and conditions of the latter are explained in the evolution management document [13].

The need of "*non-interference rules between cyber-secure and non- cyber-secure functions*" is an anticipation on the fact that to be the most secure possible, the SuC will obviously need frequent and likely urgent updates or patches to counter potential cyber-attacks. This must be performed much quicker than any other type of modifications (i.e. on safe and non-safe partitions). Therefore, as for non-safe functionalities, the latter must be without impact on the safe one to avoid the re-opening of the safety case for such type of evolutions. This makes sense as the voluntary certification activities for cybersecurity are expected to be part of a separated certificate as mentioned in the TS 50701 [27] to avoid side effect between safety and cybersecurity. Nevertheless, the strategy to define the evolution management of cybersecurity activities will be defined with the participation of the dedicated OCORA workstream (i.e. TWS06). This is identified with the brown arrow on **Figure 6**.

This should help all railway actors involved in the CCS-OB system realisation to get an easier and cheaper way to handle evolutions during its lifetime.

5.2.2.3 Configuration management

One of the major goals of OCORA is to deploy updates on the CCS-OB constituents in a faster and larger scale as it is realised today. Indeed, in the current CCS-OB system, updates are most of the time performed manually by the maintainer on each CCS-OB equipment by collecting locally a maintenance computer to the system. Without an innovative and efficient update and configuration harmonised process, the present evolution management would lose a significant part of its potential of future "game changer".

To reach that goal, OCORA supports investigations started in OCORA R3 to allow safe and secure over the air updates of the building blocks, likely when the trains will be in the depot after the train journey. The process to manage this update process will be defined in a future release of OCORA. This will be realised in coordination with the TWS08 – MDCM and the TWS06 – Cybersecurity team in R4 where a first idea of an operation process has been defined in [18].

5.2.2.4 Summary

As a summary, the benefits for the user when implementing the OCORA evolution management process would be:

- a systematic approach possible thanks to the genericness OCORA modular architecture;
- faster impact analyses (i.e. design, testing and safety) with a bottom-up approach;
- faster non-regression testing activities with predefined scopes provided by OCORA Testing team (TWS09);
- faster risk assessments following CSM-RA [33];
- faster ISA assessments thanks to the different shades of certification;
- Cost saving without degrading safety because of rationalisation of the overall change management process at project level (i.e. limitation of the "Domino's effect" propagation through the whole railway system);
- an innovative process allowing to deploy the building blocks software updates with a standardised safe and secured over the air process.

5.3 Optimised Approval Process

5.3.1 Context

The current framework for the approval of CCS Onboard systems is defined in the current European official documentation and directives (e.g. Directive 2018/545 [36]). However, it has been noted that many Railway Undertakings consider the current approval process to be quite lengthy and complex, in particular when it comes to authorising modified CCS systems, for which often all safety and approval activities have to be started from scratch again.

5.3.2 Purpose

It is the intention of OCORA to propose in the future an optimised approval process that takes advantage of the OCORA modularity to reduce efforts and time for risk assessment, safety demonstration, safety assessment and ultimately approval of OCORA components, by reusing as much as possible components or building blocks that have already been certified. The optimised approval process will apply or elaborate on concepts already existing in the standards (e.g generic product and application safety cases in EN 50129) as well as in regulations (e.g the “reference system” of the CSM-RA [33]) to achieve this objective.

As part of Release 2 OCORA has issued a document called “Discussion on Optimized Approval Process” [15] which introduces arguments for proposing a new approval process, based on an analysis of the current homologation process and an analysis of the current difficulties encountered with approving new or modified CCS on board systems. A proposal for an optimised approval process shall be developed and presented in future OCORA releases.

5.4 OCORA Certification

5.4.1 Context

OCORA compliant elements (e.g. CCS on-board, building blocks) shall be defined according to TSI CCS [20] which states the following safety requirements in section 4.2.1.1:

The CCS On-board and Trackside subsystems shall respect the requirements for ETCS equipment and installations stated in this TSI [20].

For the hazard ‘exceeding speed and/or distance limits advised to ETCS’ the tolerable rate (THR) is 10^{-9} h^{-1} for random failures, for on-board ETCS and for trackside ETCS. (See Annex A 4.2.1 a. of the TSI CCS [20]).

To achieve interoperability, the on-board ETCS shall fully respect all requirements specified in Annex A 4.2.1. Nevertheless, less stringent safety requirements are acceptable for trackside ETCS provided that, in combination with TSI-compliant CCS On-board subsystems, the safety level for the service is met.

Furthermore, the TSI CCS refers to the mandatory standards which must be complied with for CCS subsystems/components: the standards listed in the table below shall be applied in the certification process, without prejudice for the provisions of Chapter 4 and Chapter 6 of this TSI.

No	*Reference*	*Document name and comments*	*Version*	*Note*
A1	*EN 50126*	*Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*	*1999*	*1*
A2	*EN 50128*	*Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*	*2001 or 2011*	
A3	*EN 50129*	*Railway applications — Communication, signalling and processing systems — Safety related electronic systems for Signalling*	*2003*	*1*
A4	*EN 50159*	*Railway applications — Communication, signalling and processing systems*	*2010*	*1*

Table 2 List of mandatory standards

Note 1: this standard is harmonised, see Commission communication in the framework of the implementation of the Directive 2016/797/EC [37], where also published editorial corrigenda are indicated.

Based on this statement, any OCORA compliant element shall be assessed through:

- ISA for compliance with CENELEC standards (i.e. A1 to A4) or/and AsBo (Assessment Body) for compliance with CSM-RA [33] (in case of significant changes to the Railway System). Note: the two assessments can be combined and performed by the same body, provided it has the adequate accreditation for performing both assessments. Typically, though not necessary always, an AsBo is expected to be contracted by an operator (RU or IM) while an ISA is expected to be contracted by a supplier;
- NoBo (Notified Body) for compliance with TSI (i.e. compliance to the TSI and all mandatory subsets of the "*Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)*";
- DeBo (Designated Body) for compliance with National Technical Rules (NTR) in case specific NTR (available on ERA's website) apply to the system under consideration (e.g. STM, ETCS application customization for a dedicated country).

Evidence of all these assessments constitutes mandatory documentation for the approval of CCS interoperable systems.

5.4.2 Purpose

Besides the TSI certification, OCORA compliant systems should need an additional certificate that ensures that the OCORA Collaboration's set of requirements has been successfully applied in their design. This becomes mandatory for any manufacturer that wants to sell OCORA compliant standalone systems. The *CCS-OB Builder* also needs to be sure that the systems he is buying are ready for safe integration. Without this, the overall concept of modularity, exchangeability and scalability would not be efficient.

5.4.2.1 OCORA compliant projects/programs certification

OCORA Collaboration will stick to the framework defined in the European official documentation and directives with respect to the approval/authorisation process. Based on this, it is proposed to define in future OCORA releases an "OCORA certification" scheme, taking inspiration from the NoBo certification process currently used by all interoperable subsystems and constituents. However, it seems realistic to expect that there will be no European directive dedicated to OCORA, at least for the first years of OCORA deployment in the industry. This means that OCORA compliance will not benefit from a mandatory regulation as it is the case today for interoperable systems. Knowing this, OCORA Collaboration proposes that OCORA certification will be done through a parallel channel independent of the NoBo, DeBo and AsBo ones, without a mandatory regulation behind (refer to **Figure 7**).

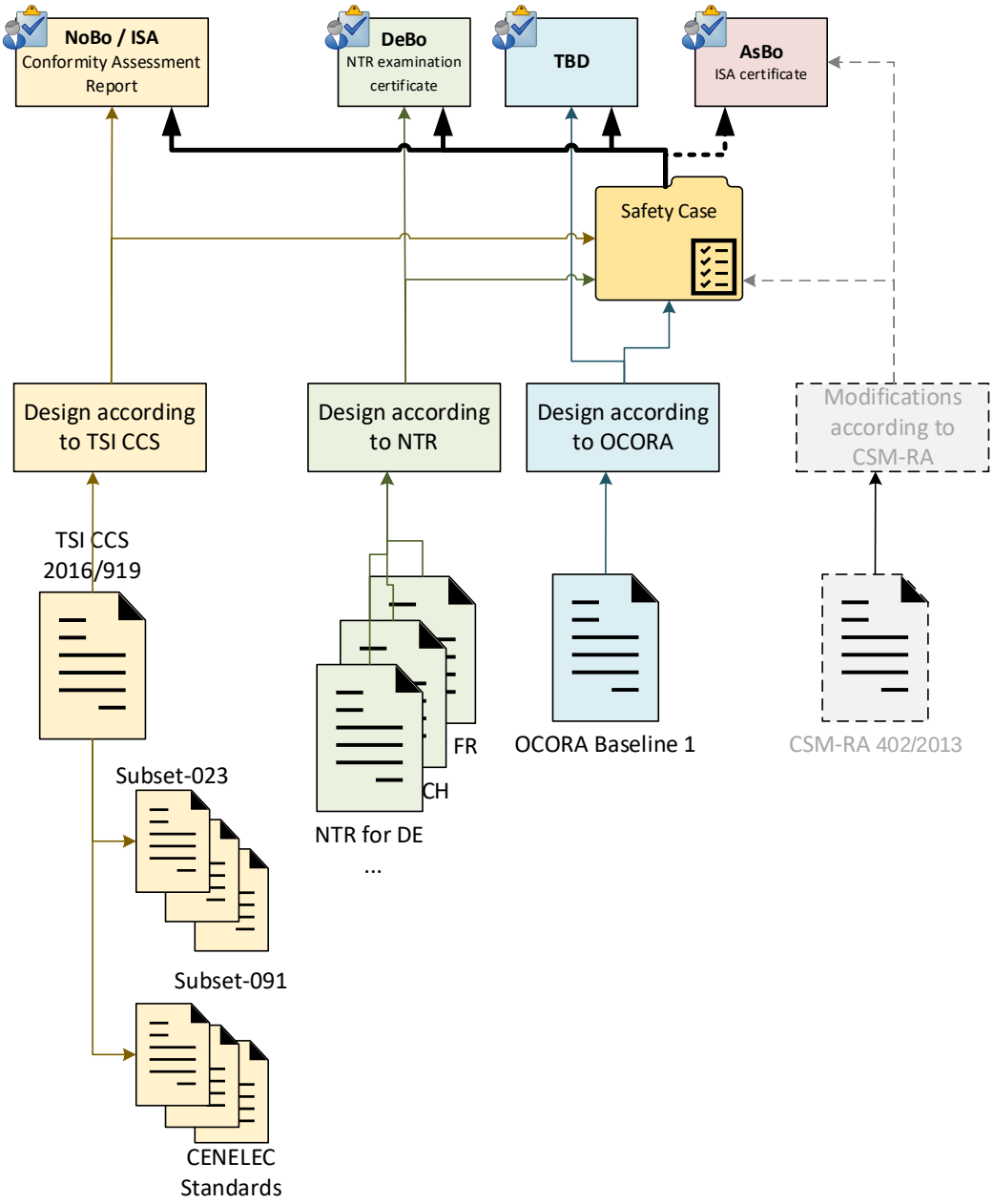


Figure 7 Regulation impacting OCORA compliant systems

5.4.2.2 Cross acceptance

Within OCORA Collaboration, two different kinds of cross acceptance are to be considered. The first one is related to the cross-acceptance of already certified products by different safety standards (e.g. IEC 61508, DO178C, ISO 2626-2). This topic is currently handled by a dedicated team (i.e. Acceptance of Global Standards) within OCORA Collaboration and the work is on-going so far [8].

The second cross acceptance topic is towards the railway market itself. Although the former EN 50506-1 [26] defines rules to perform cross-acceptance with already certified systems (i.e. GPSC or GASC only) its direct application in today's systems is not that smooth. It is common that an ISA challenges an organisation using already certified railway elements from other ISA (i.e. different companies). One of the reasons is that the responsibilities in case of reuse of cross-accepted products is not clearly stated in the standard.

However, efficient cross-acceptance is a mandatory key element to reach the benefits of a modular architecture. This point is an important topic to be handled in the next releases of OCORA as part of the optimised approval process (see section 5.3).

5.4.2.3 OCORA project documentation

The proposition is to define OCORA documentation the same way as the TSI CCS application guide is built [32]. This means that OCORA documentation for procurement will be organised as an application guide, that introduces OCORA, provides a road map for OCORA compliant projects/programs deployment and makes the links with:

- all technical specifications (i.e. future OCORA subsets);
- all workstreams processes documents (e.g. the present document, testing strategy [19]);
- any release document managed outside of OCORA that is neither called in the TSI CCS [28] or its application guide [32] but mandatory for OCORA deployment (e.g. RCA, Shift2Rail documents).

The complete documentation architecture requested through the different assessment types is presented on **Figure 8**. A dashed link is proposed between the TSI CCS [28] and the OCORA application guide. The intention is only to create a connexion but not an interdependence. This is already the case today with the application guide which is introduced through two notes for the Set of specifications # 3:

Note 4: Index 48 refers only to test cases for GSM-R mobile equipment. It is kept 'reserved' for the time being. The application guide will contain a catalogue of available harmonised test cases for the assessment of mobile equipment and networks, according to the steps indicated in point 6.1.2 of this TSI.

Note 12: Reference to these specifications will be published in the Application Guide, waiting for clarifications on the rolling stock side of the interface.

Then, trained assessors (e.g. already accredited as NoBo, AsBo) through OCORA documentation can provide a dedicated examination report. This means that the OCORA examination report template shall be based on the content of the NoBo one.

It must be noticed that any manufacturer or integrator claiming to be compliant with OCORA needs to get this "OCORA examination report". This will be a mandatory request during the call for tender from the contracting entity.

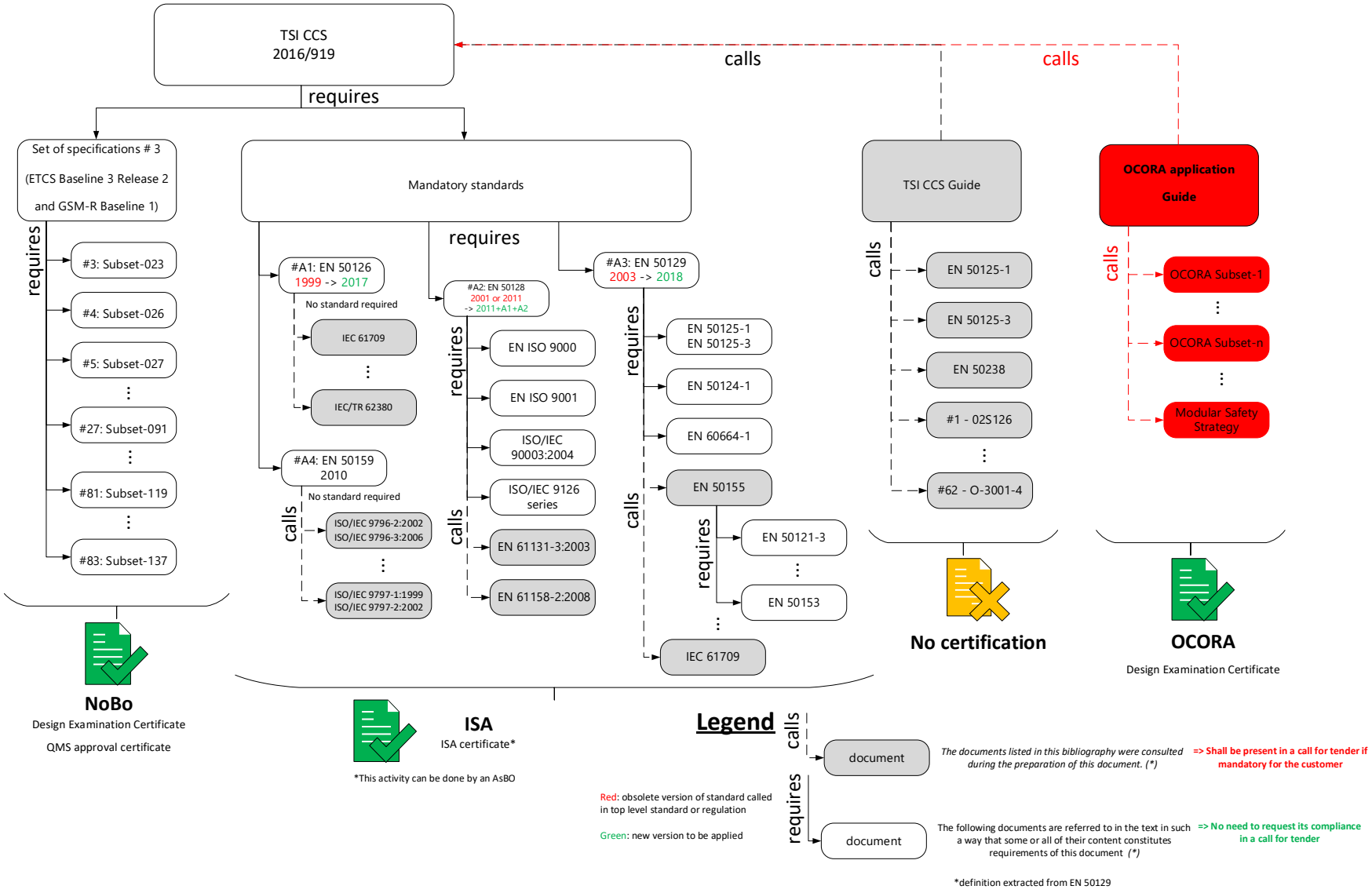


Figure 8 Documentation architecture for OCORA compliant projects

6 Safety Case Management within CENELEC documentation

This section defines the Safety Case management when dealing with a modular architecture for CCS-OB systems and is an outlook on the output of OCORA CENELEC documentation, introduced in [17].

An important point when working with a modular architecture is to define a limited list of possible safety cases to improve the genericity of their interdependence and have the integration the less complex possible. Nevertheless, it is also paramount to not freeze this safety cases list and leave some space to the *contracting entities* to define their own safety case nesting depending on the national rules and economic strategy. Furthermore, for managing the OCORA safety cases a centralised organisation is needed. These aspects are discussed in in 6.2 based on the Safety case definition in 6.1.

From an overall point of view Figure 9 presents the main levels of safety cases involved into OCORA compliant projects/programs.

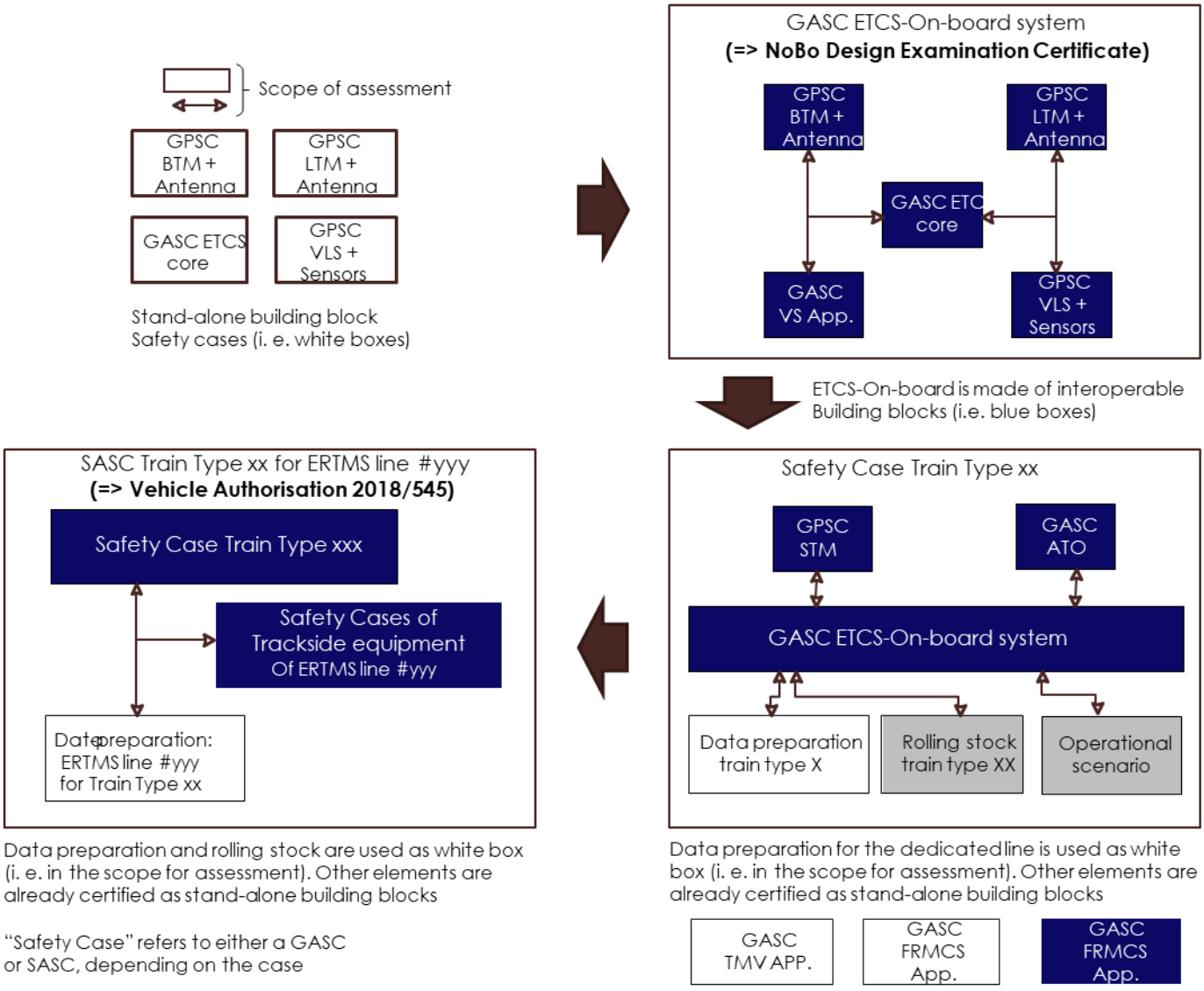


Figure 9 OCORA imbrication of Safety Cases

6.1 Safety Cases definition

6.1.1 Legacy

The starting point when building an OCORA compliant CCS-OB system is to choose the most elementary pieces that constitute it. The starting point to define them relies on the existing UNISIG documentation. From a safety point of view, Subset-091 [30], based on Subset-088-3 [29], provides safety critical items (e.g. hazards, quantified targets) for the functional blocks of the ETCS on-board constituents. This is summarised in **Figure 10**.

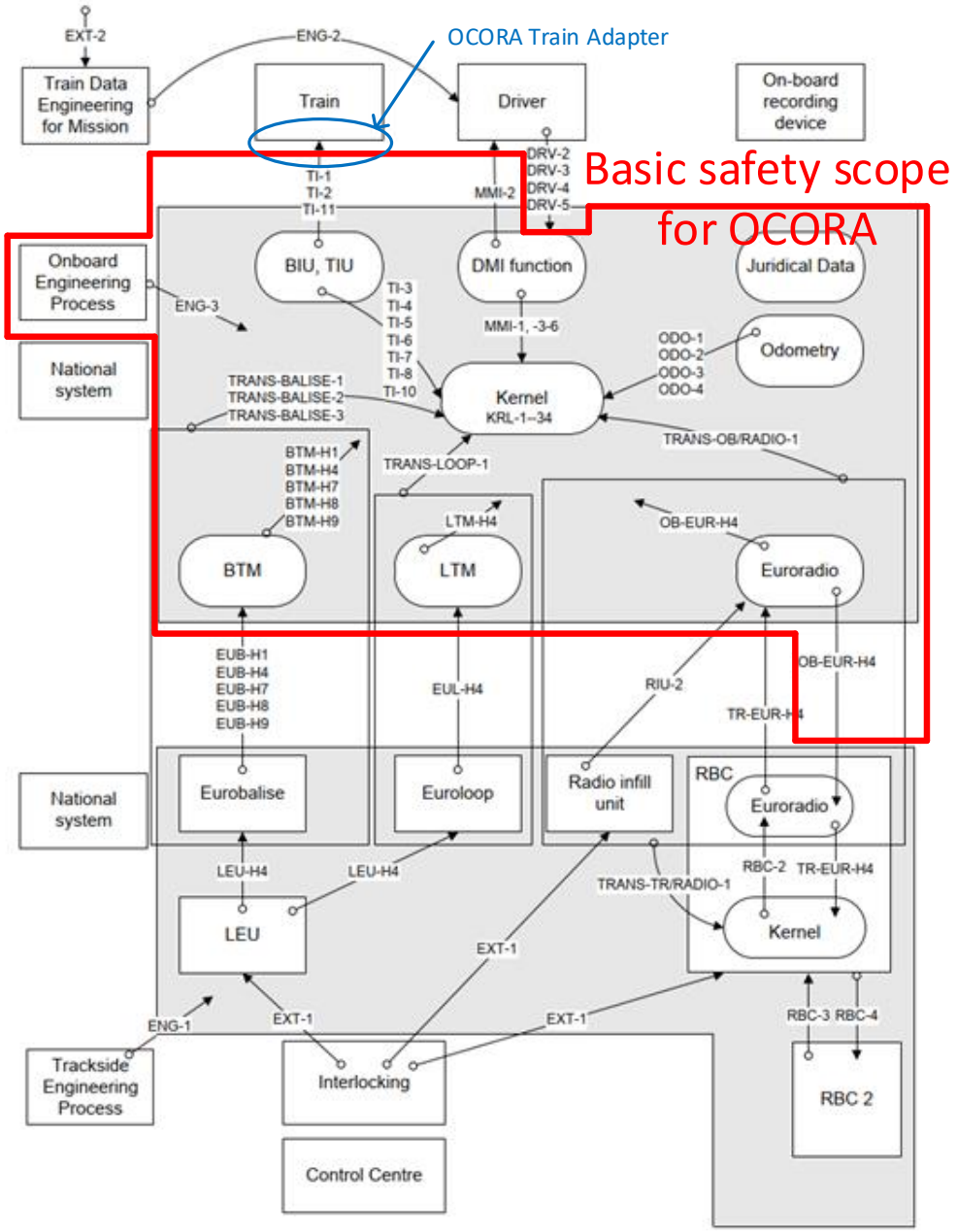


Figure 10 OCORA functional safety scope (i.e. ETCS on-board)

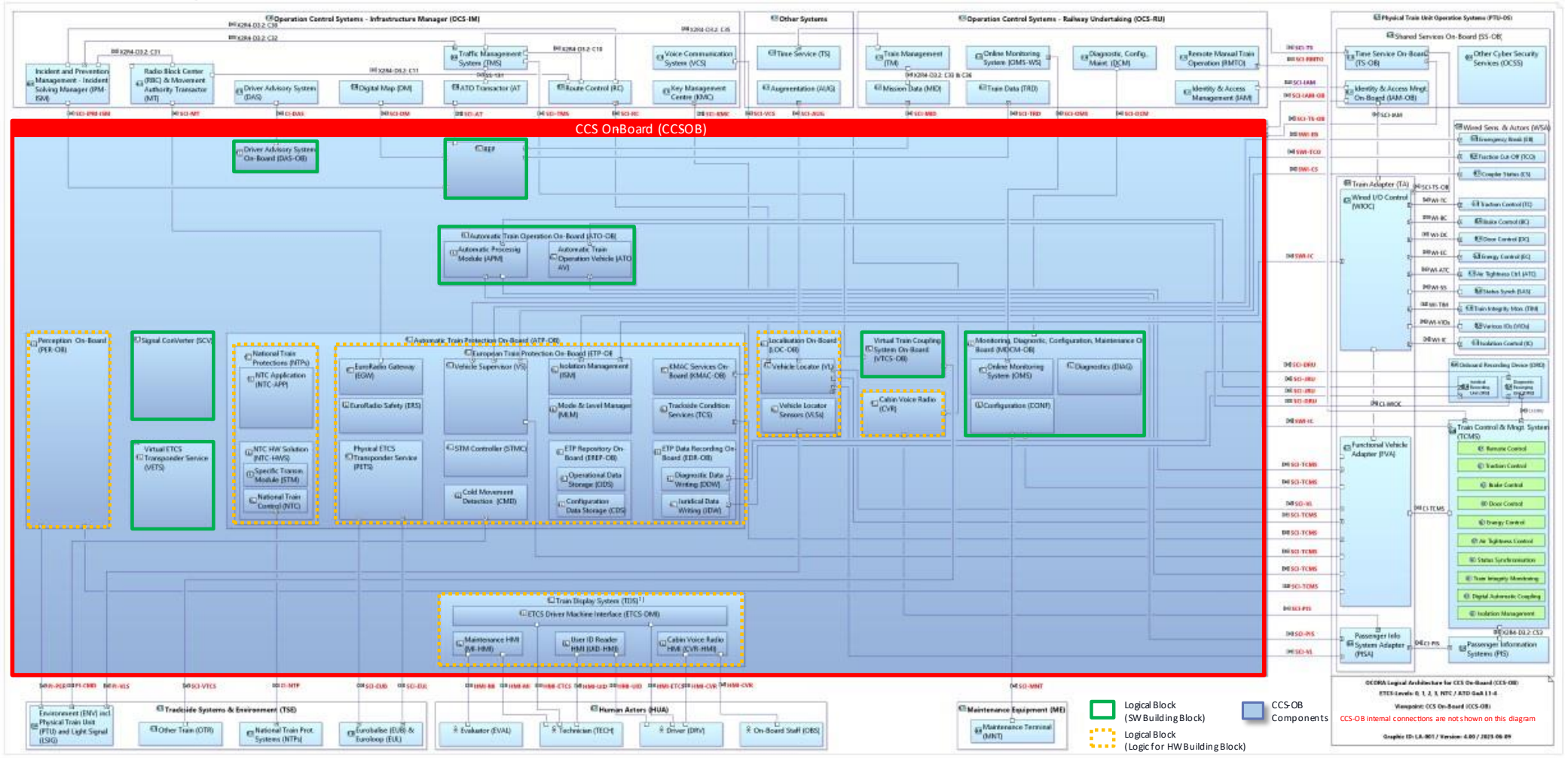
6.1.2 Implementation within OCORA Collaboration

A complete analysis of the latest releases of these two subsets shall be performed by OCORA release. The goal is to identify if their safety data is sufficient to realise standalone safety cases for the building blocks. OCORA Collaboration has identified some lacks in the current documentation and provide the missing data in a future, updated version of this document. This analysis will be used by the OCORA Architects to finalise the definition of the OCORA building blocks. The idea behind this is to stick as close as possible to the already well-known existing systems to avoid a complete rebuilt from the suppliers which would lead to a major conflict. Thus, any time a safety data such as THR is provided for a function, it shall be reused by OCORA.

During R1, the RAMS team analysed Subset-088 [29] and 091 [30] without success. Without access to the complete safety analyses used to build these subsets (e.g. FTA files) it is impossible to find out the target for each elementary hazard identified in Subset-091 [30]. This activity will be realised inside the ERJU Innovation Pillar with the collaboration of the UNISIG that hosts these safety analyses.

A first proposition for the building blocks is already defined in OCORA Architecture [10] and shown on **Figure 11**.

External Logical Interfaces(Legacy Train Example)



1) TDS-OB may be moved into the PTU-OS / LOC&PAS domain.

Figure 11 OCORA building blocks as presented in the OCORA architecture of R4

This list of building blocks is the final proposition by OCORA and must be now agreed with industrial partners (e.g. UNIFE, UNISIG). The latter, when validated, will be exhaustive, and the building blocks scope, borders and SRAC cannot be modified by a supplier. This is to ensure interoperability (i.e. TSI [28] CCS and OCORA) between different vendors. As mentioned in Assessment activities, each vendor is responsible of managing the required certifications processes.

A particular focus is made on the:

- use of the standardised SRAC defined by the OCORA Collaboration and present in the document SRAC management guideline (ref [14]);
- use of vendor specific SRAC (if any) only where no conflict with OCORA one is possible;
- conformity to OCORA SRAC management guideline is demonstrated.

The SRAC management through OCORA is presented in section 5.1.

6.2 OCORA Safety Cases integration

6.2.1 Context

ERA defined the concept of *safe integration* and has defined activities to be realised any time a stakeholder is composing a whole system based on the integration of smaller sub-systems.

The construction of any new equipment composed of multiple smaller parts, or the introduction of a new or a modified element into an existing system, is a common development activity. Regardless of the level at which such development takes place, safe integration is necessary at every level to ensure the safe achievement of the expected functionality and to demonstrate that the change does not create unintended, adverse and unacceptable effects on the safety of the overall system.

The previous statement is extracted from [34]. It is represented on **Figure 12**.

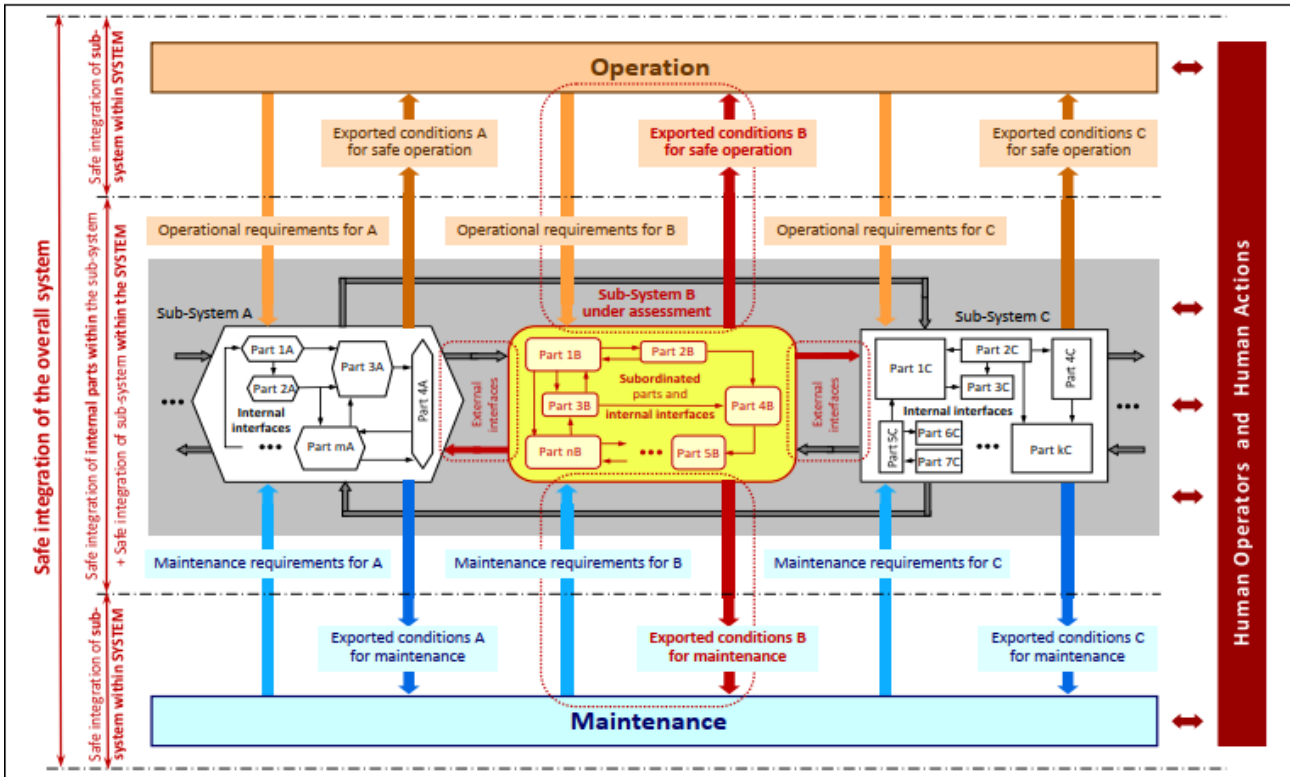


Figure 12 *Different levels of safe integration within the architecture of a system* from [34]

Figure 12 presents a relevant generic vision of sub-systems (i.e. building blocks) integrated in an overall system (e.g. CCS-OB system). All these interactions must be addressed within the OCORA compliant project/program. **Figure 13** provides a concrete application of the integrated system under consideration when dealing with OCORA. From **Figure 12**, it must be understood that:

- Maintenance requirements
- Exported conditions for maintenance
- Operational requirements (refer to [12] for OCORA)
- Exported conditions for safe operation
- External interfaces (requirements)

are requirements that will be published by the OCORA Collaboration, as well as the technical requirements for the newly defined internal interfaces of the CCS-OB system.

6.2.2 Implementation in OCORA Collaboration

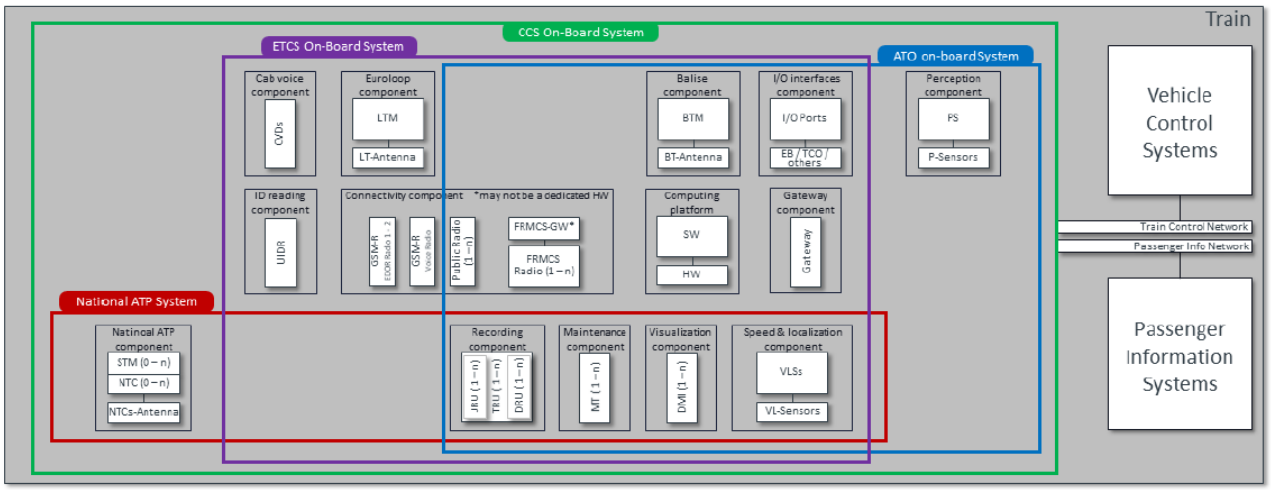


Figure 13 CCS-OB Subsystems Overview

OCORA Collaboration covers topics for the whole CCS-OB system as defined by the TSI CCS [28]. However, as presented on **Figure 13**, different other systems (i.e. all within the CCS-OB one) exist.

- **National ATP System** refer to Class B systems listed in [35] which are compatible with STM interfaces defined in the related TSI Subsets.
- **ATO on-board system** refers to the ATO new functionality introduced in TSI 2022. The dedicated modules are expected to be non-safety related for the TSI 2022 in Subset 125, 143 and 147. Regarding this, it is out of purpose for the OCORA Modular Safety document.
- **ETCS on-board system** (i.e. scope of the current TSI Subsets) composed of all ERTMS interoperable components, safety related or not (e.g. BTM, LTM, DMI, JRU, TRU, EURORADIO).
- **CCS on board system** oversees the three above systems. This is the widest scope possible for an OCORA compliant project/program.

Based on the description above, only the ETCS and CCS-OB systems are considered when dealing with integrated safety cases involving OCORA. The same strategy as for the standalone building blocks safety cases will be followed for the integrated safety cases. This means that regarding the whole safety target allocated to the CCS-OB system, the use of existing safety data coming from Subset-091 [30] and Subset-088-3 [29] will be reused every time it is possible. OCORA Collaboration will only provide safety data (e.g. hazards, targets) where it is missing. Again, this is to avoid unnecessary system incompatibilities with already existing solutions.

The decision of realising a safety case at CCS and/or ETCS level relies on:

- the strategy put in place by the contracting entity (see **Figure 14** and **Figure 15**);
- the homologation rules in place in the member state of the applicant. Indeed, for some countries, the safety evidences will be mandatory at ETCS on-board level whereas for others an overall CCS-OB safety case will be expected. Sometimes, intermediates safety cases may also be required.

Whatever the case, the modular approach proposed by OCORA brings flexibility and allows to easily (i.e. without too much costs and delay effort) increase the scope from ETCS to CCS if required.

6.2.3 Examples of future project architecture

To help the reader understand how a contracting entity can deploy this safety case management through different fleets he has to equip, two examples (not based on existing solutions) are proposed.

Figure 14 and **Figure 15** present the FVA tightened to the different type of trains although they are in the scope of OCORA. Nevertheless, they are not in the CCS-OB scope as defined in [11]. Today, it seems realistic that each rolling stock supplier is the most relevant organisation for delivering the FVA of each vehicle type as the latter embed proprietary interfaces. Therefore, from a safety case point of view, it makes sense to integrate them when realising the train type safety case.

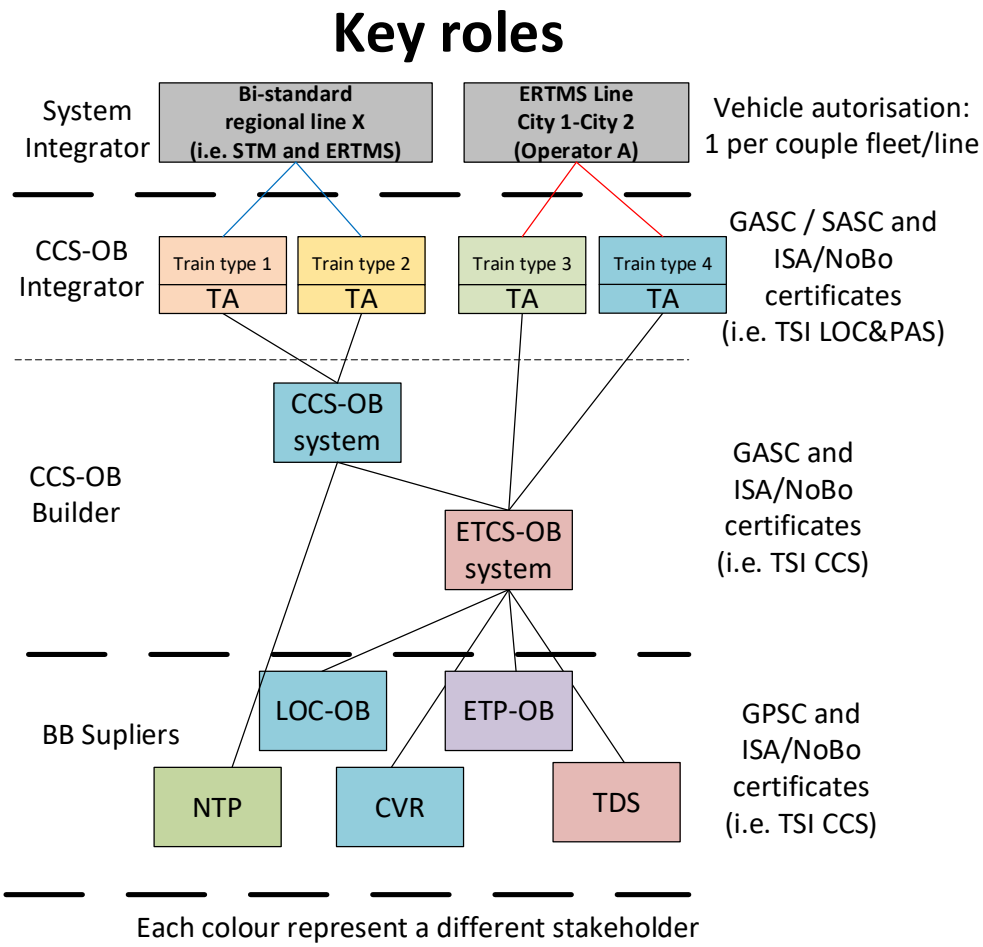


Figure 14 Example 1 of an overall fleet newly defined or retrofitted

Figure 14 presents an example of four new (or retrofitted) vehicle authorisations for two different networks. It must be noticed that the network elements are not presented on the two pictures.

To equip these four fleets, two different systems are required:

- ETCS on-board system for the ERTMS line;
- CCS-OB system for the bi-standard (i.e. both KER from [35] and ERTMS).

The CCS-OB system integrates the ETCS on-board system that equips the fleets to be deployed on the ERTMS line plus a STM allowing to handle the KER balises.

Within this architecture, the CCS-OB system completely reuses the ETCS on-board one without modifications (beside the parameters related to the safe integration of the vehicles with the network). This means that the safety activities to be deployed at CCS level will be very much limited to the validation of the STM interfaces with the ETCS on-board system and the rolling stock (i.e. the STM is delivered with its own ISA/NoBo certificates).

The benefits of deploying an OCORA compliant architecture will be visible when managing the future assessments at ETCS and CCS-OB levels following evolutions.

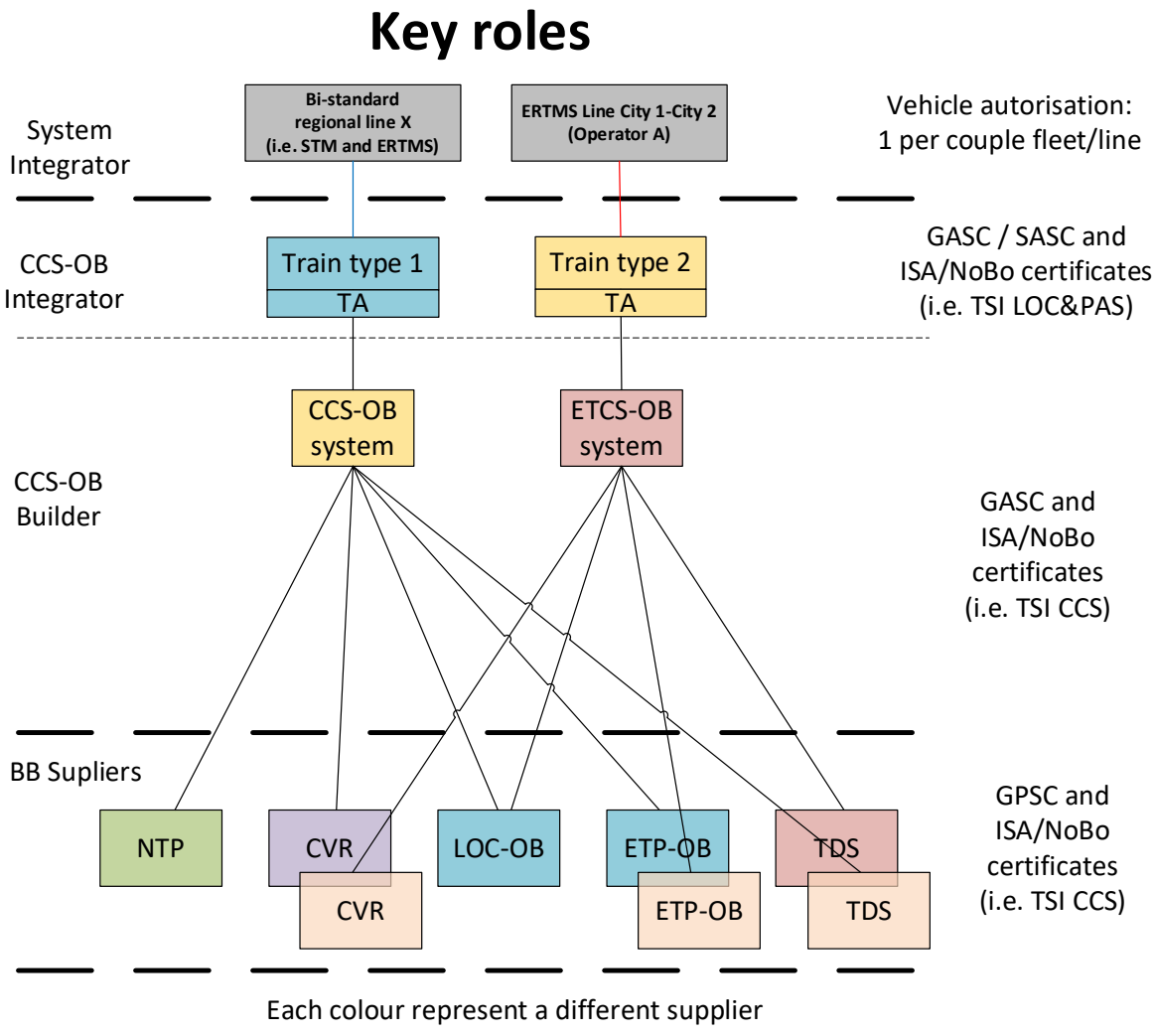


Figure 15 Example 2 of an overall fleet newly defined or retrofitted

Figure 15 presents a different strategy than on **Figure 14**. In that case, the contracting entity has chosen to define two independent systems made of building blocks from different suppliers.

The final goal is identical to **Figure 14** :

- a fleet running on a bi-standard line equipped with a CCS-OB system (i.e. included a STM);
- a fleet running on an ERTMS line equipped with an ETCS on-board system.

The benefit of this schema is that when realising the two systems, anytime two sources of equipment are used (e.g. ETCS core, BTM), mixing configurations can be tested during their first assessment. Thus, for the future ones, no tests would be required when switching between the different brands equipments. This aims at improving the availability of the overall system by allowing different sources of spare parts. Indeed, either the ETCS on CCS-OB system can be updated with any of the already tested source of components as spare parts without any assessment costs and commissioning delay. The *contracting entity* is thus not struggled with usual long delays to get new spare elements from a manufacturer.

The benefits will show up in case of evolutions or maintenance activities of the CCS and ETCS on board systems after a first assessment is successfully performed.

6.2.4 Need for a centralized organisation

The OCORA RAMS team sees the need for establishing a centralised organisation for managing and validating the safety cases for an OCORA compliant CCS-OB system.

This organisation shall:

- define and update the RAMS requirements for OCORA compliant building blocks;
- define and update templates and process descriptions (e. g. for AC management);
- define and update guidelines for testing and validation within the development of OCORA compliant building blocks;
- check conformity of CCS-OB safety cases to OCORA specifications and grant certificates.

As stated already in section 3.2, parts of OCORA will be integrated in the recently established ERJU. The idea and the development of this proposed centralised organisation can be developed within the PRAMSS work stream of EU-Rail’s System Pillar.