OCORA

Open CCS On-board Reference Architecture

Modular Safety Strategy

Document ID: OCORA-TWS07-010

Version: 1.03

Release: Delta

Date: 30.06.2021

Revision history

Version	Change Description	Initial	Date of change
1.03	Official version for OCORA Delta Release	JB	30.06.2021

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-40-012-Gamma – Modular Safety – Whitepaper

[13] OCORA-TWS01-910 CENELEC Phase 1 – Concept

[14] OCORA-TWS05-020 – Stakeholder Requirements

[15] OCORA-TWS09-010 - Testing Strategy

[16] 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

[17] RCA.Doc.11, Chapter Modular Safety – v1.0

[18] RCA Modular Safety – PowerPoint from Steffen Schmidt

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

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

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

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

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

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

[25] 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

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

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

[28] 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

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

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

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

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

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

1 Introduction

1.1 Document context and purpose

This document is published as part of the OCORA delta release, together with the documents listed in the release notes [1]. It is the first release of this document and it is still in a preliminary state.

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 on-board system as defined in TSI CCS [16]. A focus is done on the following topics:

- Introduction to Modular Safety,
- OCORA ,
- Safety Cases management,
- Evolutions management,
- Assessment management

The modular safety strategy is evolving in parallel with other OCORA workstreams (e.g. Testing, FVA, Platform,…), 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 realize the official set of documents that will be finally used by the industry and railway operators for the call for tenders for new CCS on-board systems. A more detailed presentation is provided in the OCORA Concept [13]. The present document has been realized by the Modular Safety team, identified as TWS07 within OCORA Collaboration. This team involves safety managers from the companies involved into OCORA with different skills and background to benefit of a large scope of return of experience.

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

This document is addressed to safety managers that are involved into the realization of OCORA compliant ETCS or CCS on-board systems acting as contracting entities, 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 delta release documentation can be given by using the feedback form [2].

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 this documents are issued. The Modular Safety whitepaper [12], issued in Gamma release 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

This section aims at defining what is commonly called “Modular Safety” in the context of OCORA. Some hints have already been presented in RCA through [17] and [18] and in the OCORA whitepaper [12]. 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 onboard systems. 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 becomes a complexity 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 onboard 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 onboard system does not evolve as it is expected over its lifetime. This makes economic viability of the CCS onboard system low.

A modular safety approach will allow a much easier evolution of the CCS on-board 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 standardized interfaces) will also avoid vendor lock-in caused by the intertwining of the CCS onboard modules. This avoidance makes railway undertakings more flexible in suppliers.

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

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

Modular Safety takes advantages and support the modular architecture of the OCORA initiative: safety activities are based on an architecture made by modular building blocks with standardized interfaces.

Modular Safety shall support for new projects, a harmonized strategy for integrating the required building blocks composing a CCS/ETCS on-board system.

Modular Safety shall support for new and retrofit projects, 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 4.1.2.

Modular Safety shall support a harmonized strategy to allow the most possible fluent deployment of evolutions (e.g. upgrades, new functionalities) of the OCORA CCS/ETCS on-board system and its constituents reducing the certification efforts (initial- and re-certification) at all levels without degrading the safety level of the system.

Modular Safety shall also define the safety elements necessary to allow the homologation of the OCORA stand-alone building blocks and the integrated CCS/ETCS on-board system.

2.2.2 Modular Safety goals

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

fulfill 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 standardized safety application conditions (SRAC) for the building blocks, thanks to a robust interface design,
- Clear and comprehensive safety concept of the “black box” behavior, thanks to the modular target system design,
- Broad acceptance of assessors/assessment methods, thanks to a clear cross-acceptance methodology,
- Standardization 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).

2.2.3 OCORA documentation

Two different kind of documents are to be considered for the documentation:

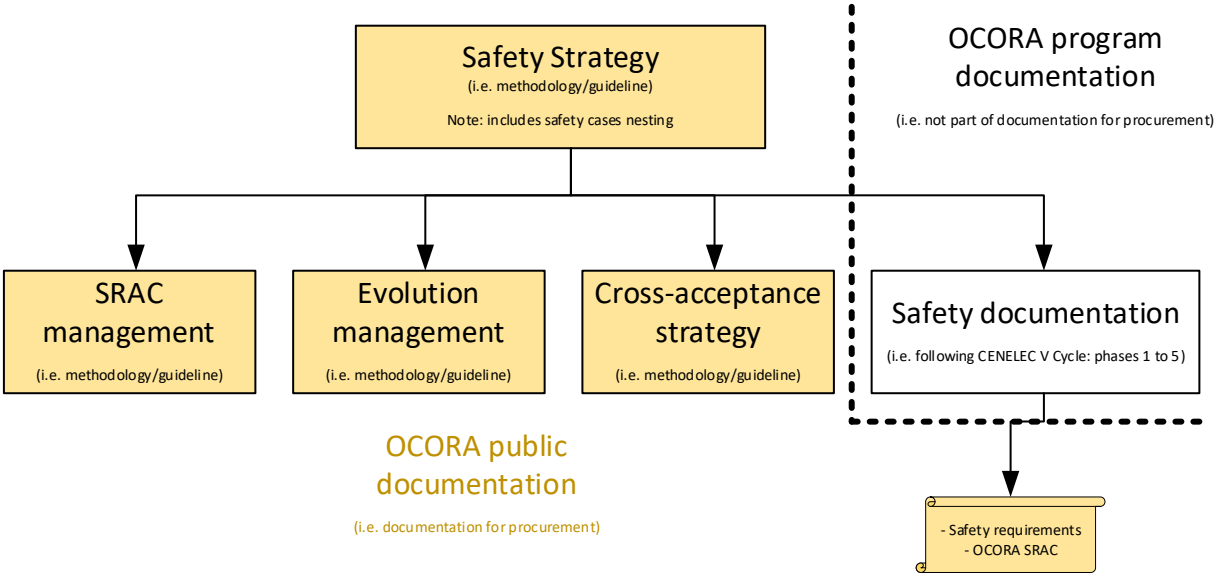

Figure 1 OCORA documentation

2.2.3.1 OCORA public documentation

The main initiative driven by the Modular Safety team will find their concrete materialization in a set of OCORA Collaboration documents and processes made at disposal to the different actors involved in the OCORA usage (i.e. yellow documents in Figure 1).

Documentation and processes in responsibility of the Modular Safety activities are provided as a “tool kit” for future projects/programs aiming at developing OCORA compliant CCS on-board systems. Some examples are identified hereafter:

- **Safety strategy guideline** (present document) to safely handle new modular CCS/ETCS systems deployment or the transition between a conventional CCS to a OCORA compliant one (i.e. retrofit),
- **Safety requirements** (including SRAC) for procurement including (not exhaustive):

- The links between CCS on-board system integration requirements, building blocks assigned requirements and SRAC,
- The flow of safety requirements from CCS on-board to building blocks levels and their assignment to the different actors,
- Hazards and quantified target for each building block.

- **A methodology for handling SRAC** (refer to section 4.3) through OCORA compliant systems. This defines, among other topics, the rules for SRAC writing and method for closing them at upper levels,
- **Process for safely handling evolutions** (refer to section 5) within an OCORA compliant system (i.e. from building block to vehicle authorizations),
- **An improved cross-acceptance process to handle assessments** (refer to section 6) for the first OCORA compliant integrated system one and later, during its lifetime when evolutions are expected.

The use of the set of documents delivered by the Modular Safety team will become mandatory for suppliers and integrators in order to finally being successfully assessed through OCORA (refer to 6.2.1).

2.2.3.2 OCORA program documentation

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 [13] (i.e. Phase 1 according to EN 50126-1 [19]). This documentation will be provided by a dedicated team within OCORA (i.e. referred as TWS01-WP09) where the members are also involved in the Modular Safety one.

The OCORA Collaboration documentation (i.e. white documents in in Figure 1) are not mandatory for the stakeholders building the future CCS on-board systems. They will be provided as informative to help and support them to realize their own development cycles. This documentation is made of (not exhaustive):

- OCORA program Management Plan: plan that oversees the OCORA program regarding logistic, planning, organization, scope topics,
- OCORA program Safety Plan: document that presents the set of activities to de deployed to develop a SIL4 system,
- OCORA program RAM Plan: document that presents the set of activities to de deployed to develop a SIL4 system,
- OCORA program Quality Plan: document that oversees the activities to ensure a suitable development and reinforce the protection against systematic failures,
- OCORA Program System Hazard Analysis: document realized in phase 4 on the system functions aiming at performing the safety analysis to identify the safety related functions,
- OCORA program Verification Plan: document presenting the verification activities to be defined for a SIL4 program development (e.g. traceability matrixes, test cases for requirements)

The complete list of OCORA Collaboration deliverables will be issued in the Safety Plan that will be realized in Phase 2 according to EN 50126-1 [19].

2.3 Barriers for Modular Safety implementation

What is hindering modular safety to be implemented and why it isn't already implemented?

Vehicle supplier act in most cases as an integrator 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 [19]) towards their suppliers. Motivation for that is based in the very same area as the OCORA objectives: enable evolution, enable inter/exchangeability, manage obsolescence, 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/ETCS 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 very 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 the distributed engineering, which results in too complex solutions, becomes hard to be understood in terms of safety (e.g. safety managers and assessors).

3 OCORA stakeholders

3.1 Context

Prior presenting the safety case nesting, clarification shall be brought to 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) 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 precised tasks and responsibilities. Furthermore, all these independent stakeholders must be managed and coordinated by an overall stakeholder that ensures the smooth communication, integration, safety data workflow between them.

In a parallel development, ERA has realized its own return of experience on the vehicle authorization process [33] because the concept of “safe integration” defined in the latter was used to be misunderstood (i.e. a limited scope of activities was deploying by the directive’s applicants).

Thus, ERA has emitted a document called ERA 1209-063 Clarification note on safe integration [31] where information is proposed to handle the “safe integration” in a generic way and also when dealing with vehicle authorizations.

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 and ERA 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 fulfill 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 2 presents the list of all railway actors for vehicles and network from a high-level point of view (i.e. vehicle authorization). 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 where only the key actors having a direct impact on modular safety and the safety workflow between them. This is presented in Figure 3

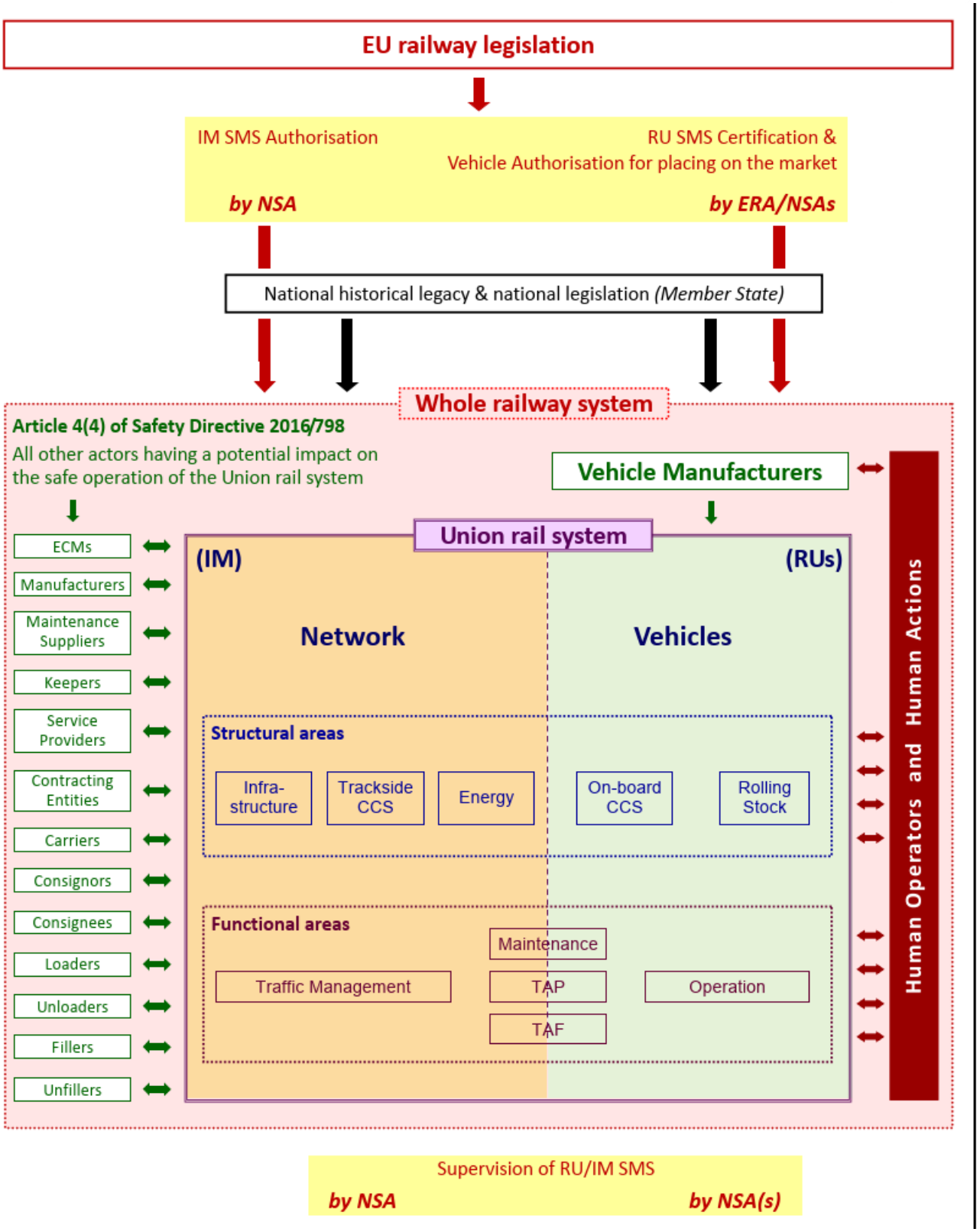

Figure 2 ERA list of railway stakeholders (from [31])

3.2 Implementation in OCORA Collaboration

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

- *On-board CCS integrator,*
- *Vehicle integrator.*

Indeed, today, the *On-board CCS integrator* is always the CCS/ETCS on-board supplier because current systems are provided as monolithic blocks, composed of proprietary elements and proprietary internal interfaces.

In addition, the *Vehicle integrator* is always the rolling stock supplier and most of the time from the same company as the CCS/ETCS on-board one.

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 *on-board CCS integrator*. The latter shall coordinate the activities of the different suppliers to integrate their sub-systems and ensure that finally, ISA and NoBo (plus DeBo and AsBo when required) certificates of the CCS/ETCS on-board system will be delivered by the assessor.

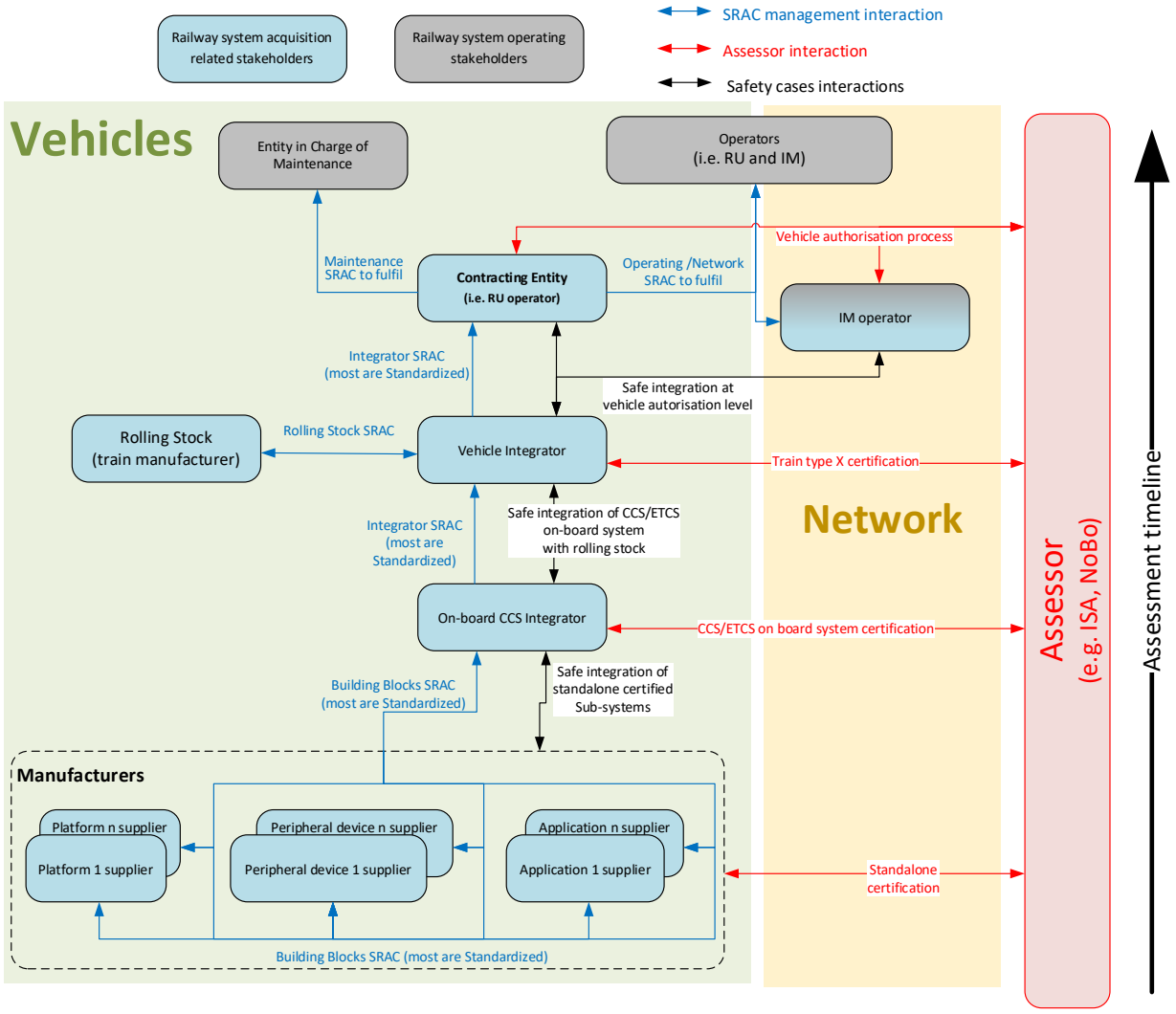

Figure 3 OCORA modular safety stakeholders

The different workflows (bottom-up) identified on Figure 3 are described hereafter:

- **Assessment activities:**
  - **Standalone certification**: one important goal of OCORA is that an integrator can build a CCS/ETCS on-board system based on different suppliers' building blocks (i.e. platforms, peripheral devices and applications of Figure 3). In ERTMS context, that means that each interoperable sub-system shall be certified as standalone part (see 6.2.1):
    - NoBo independent conformity assessment for any element defined in TSI CCS [16]
      - Interoperability certificate (i.e. design examination certificate),
      - ISA certificate (for all safety related building blocks),
    - AsBo independent conformity assessment (i.e. in case of significant change according to CSM-RA [30] at operators level),
    - DeBo examination report (when the building block deals with NTR),
    - OCORA compliance assessment report for any element defined in TSI CCS [16].

    This activity is under the responsibility of each building block's supplier.

  - **CCS/ETCS on board system certification**: this activity, led by the newly defined role in the railway world; *On-board CCS Integrator*, 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/ETCS on-board systems. The complete list of tasks and responsibilities for this kind of integrator is defined into the glossary [3].

    Based on a set of mandatory documents provided by OCORA Collaboration defined in the overall OCORA application guide, the CCS/ETCS on-board integrator shall handle the assessment panel defined in Assessment activities.

  - **Train type X certification**: this activity focuses on the integration of the CCS/ETCS on-board system (i.e. scope defined by TSI CCS [25]) inside a rolling stock equipment (i.e. scope defined by TSI LOC&PAS [28]). This activity shall be realized by the newly defined *Vehicle Integrator* whose tasks and responsibilities are defined in the glossary [3]. Its activities are already well defined and bordered thanks to the two TSI (i.e. [25] and [28]).

    Based on them and on the set of mandatory documents provided by OCORA Collaboration defined in the overall OCORA application guide (will be ready in Release 1.0), the integrator at train type level shall handle the assessment panel defined in Assessment activities.

  - **Vehicle authorization process**: this activity represents the top-level assessment where the rolling stock presents its compatibility within a dedicated network. At this level, ERA clarification note [31] 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/ETCS building blocks. This is presented in section 5.

- **SRAC flows:**

  The overall management of the SRAC in OCORA compliant projects/programs is introduced in section 4.3.

  - **Building Block SRAC (most are standardized)**: this workflow represents all different SRAC 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 on-board system will be standardized. Following that, the safety analyses performed within OCORA Collaboration on them will result in a generic set of SRAC that should be harmonized 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 Modular Safety team.

Finally, only a few SRAC will remain supplier's dependent. They concern all non-standardized 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 SRAC can be addressed to other building blocks or to an upper level of integration.

- **Maintenance SRAC to fulfil:** this workflow presents all SRAC 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 authorization process.

- **Operational /Network SRAC to fulfil:** this workflow presents all SRAC 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 authorization process.

- **Rolling Stock SRAC to fulfil**: this workflow presents all SRAC that are emitted at any level of the overall OCORA compliant project/program and provided to the rolling stock supplier by the *Vehicle Integrator*. The latter has to provide for each of them a proper coverage that will be part of the vehicle authorization process. The rolling stock supplier can also provide SRAC for some building blocks and the *Vehicle Integrator* ensures that their coverage is provided by the different involved manufacturers.

4 Safety Cases management

This section defines the Safety Case management when dealing with a modular architecture for CCS/ETCS on-board systems.

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. This is developed in 4.2

From an overall point of view, based on Figure 3 with the red arrows, Figure 4 presents the main levels of safety cases involved into OCORA compliant projects/programs.

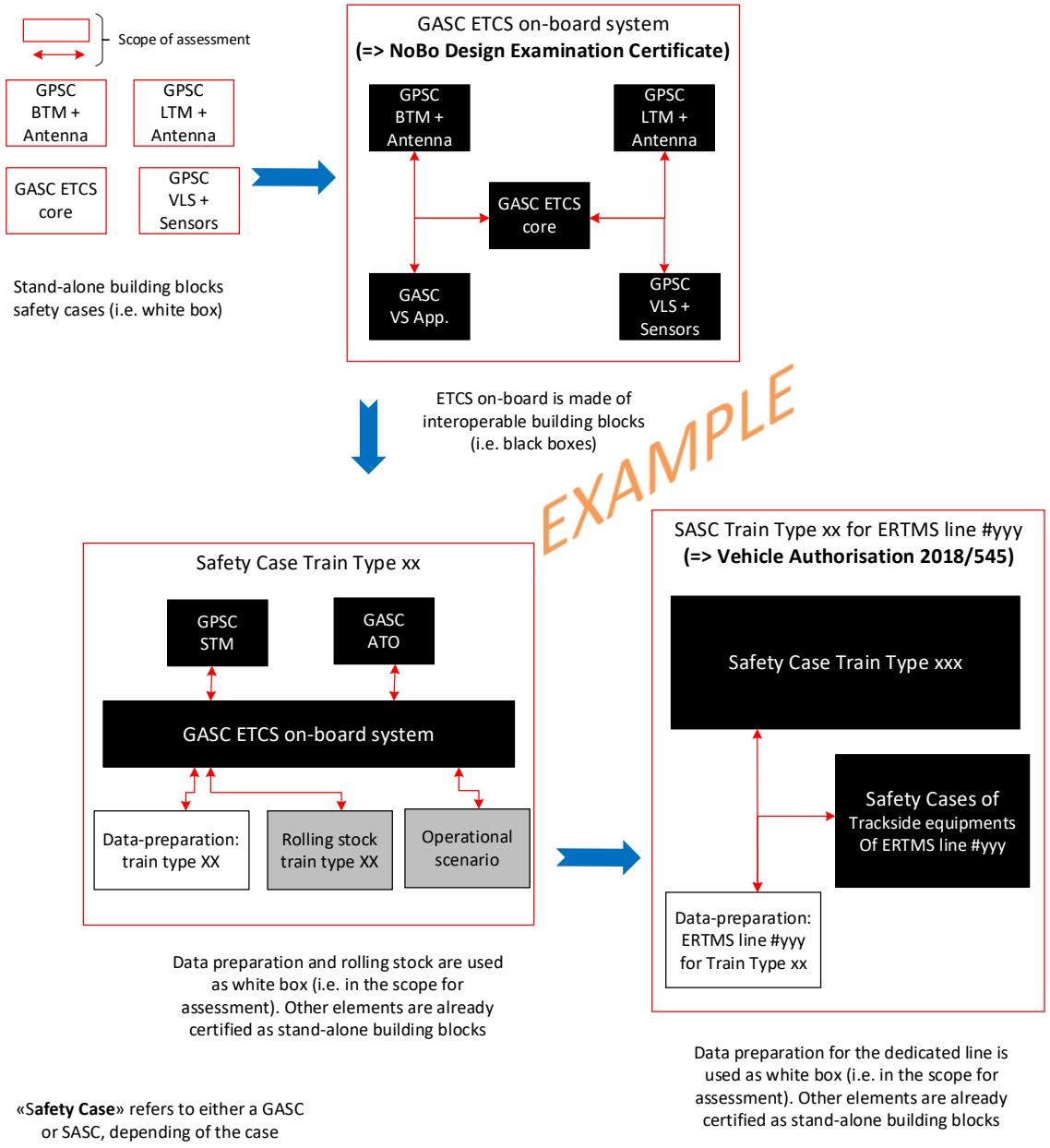

Figure 4 OCORA compliant projects/programs safety cases

4.1 OCORA Safety Cases definition

4.1.1 Legacy

The starting point when building an OCORA compliant ETCS/CCS on-board 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 [27], based on Subset-088-3 [26], provides safety critical items (e.g. hazards, quantified targets) for the functional blocks of the ETCS on-board constituents. This is summarized on Figure 5.

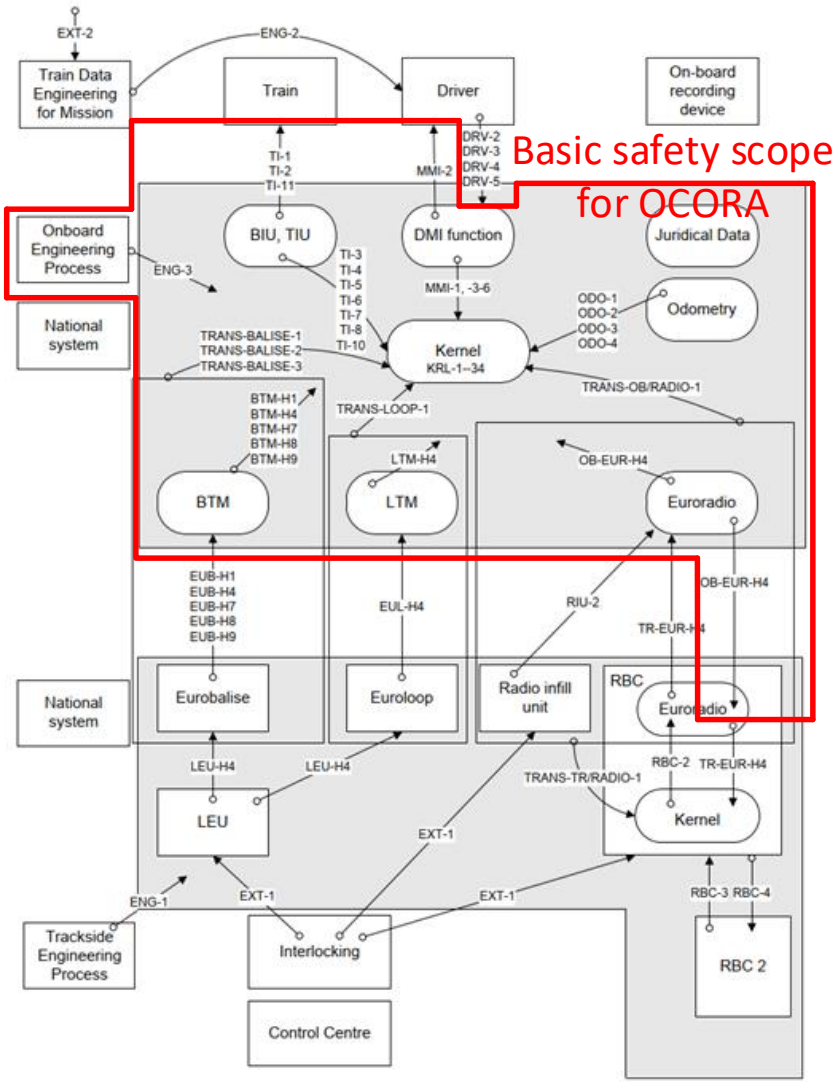

Figure 5 OCORA functional safety scope (i.e. ETCS on-board)

4.1.2 Implementation within OCORA Collaboration

A complete analysis of the latest releases of these two subsets will be performed in Delta + 1 OCORA release. The goal is to identify if their safety data is sufficient to realize 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 finalize 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.

A first proposition for the building blocks is already defined in OCORA Architecture [10] and shown on Figure 6.

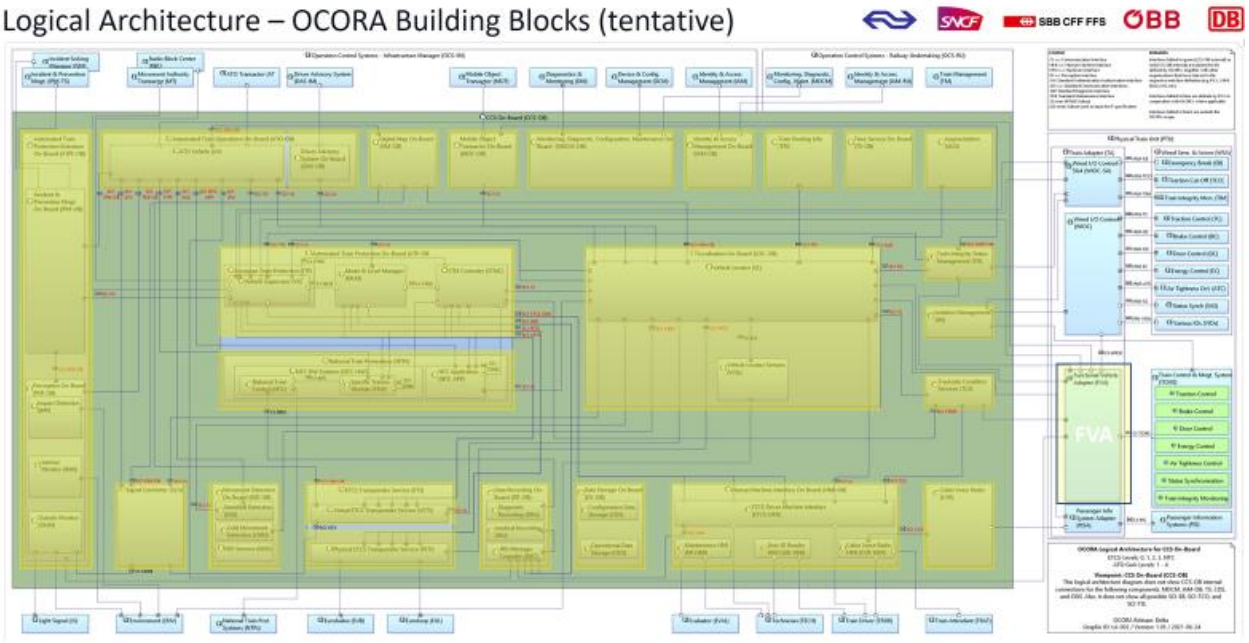

Figure 6 OCORA building blocks safety cases

The latter, when stabilized, will be exhaustive, and the building blocks scope and borders (including SRAC) cannot be modified by a supplier. This is obviously to ensure interoperability (i.e. TSI [25] 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 generic SRAC defined by the OCORA Collaboration and present in the document SRAC management guideline (will be ready in Release 1.0),
- Use of vendor specific SRAC (if any) only where no conflict with OCORA one is possible,
- Conformity to OCORA SRAC management guideline (will be ready in Release 1.0) is demonstrated.

The SRAC management through OCORA is presented in section 4.3.

4.2 OCORA Safety Cases integration

4.2.1 Context

ERA defined the concept of *safe integration* and has defined activities to be realized 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(8), 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 [31]. It is represented on Figure 7.

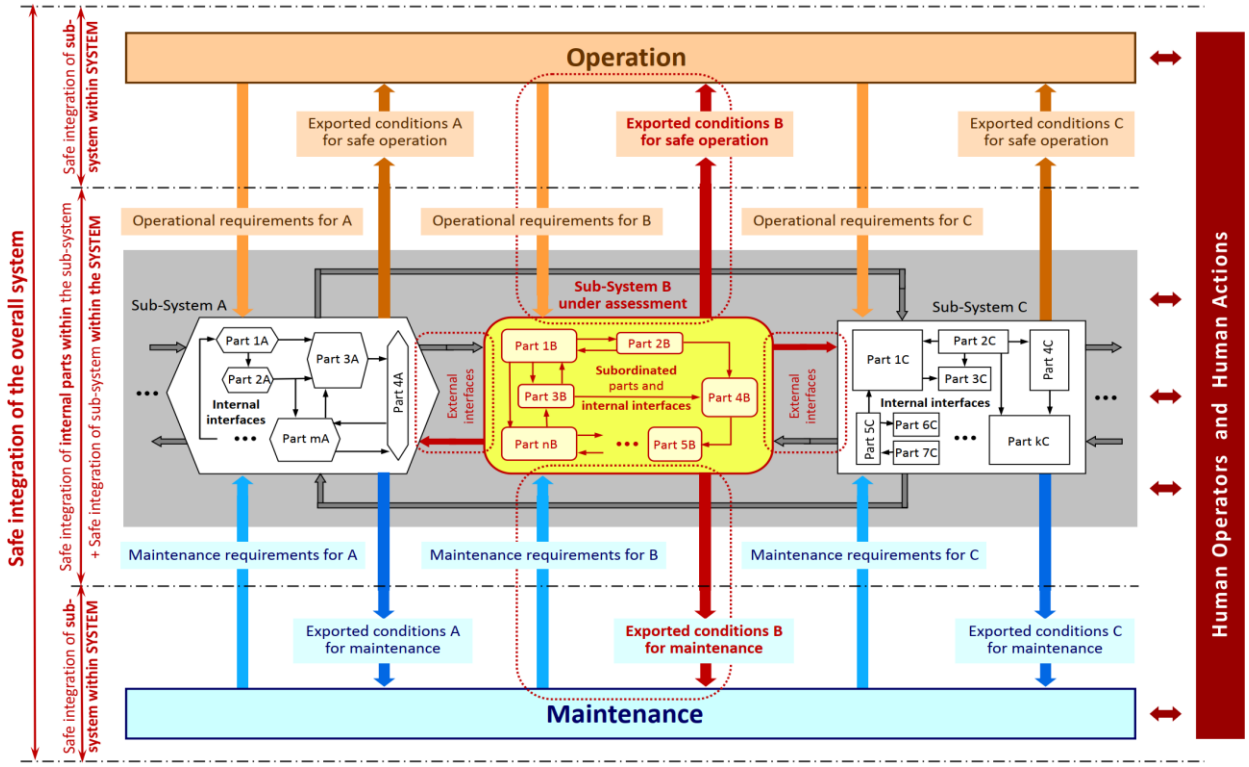

Figure 7 *Different levels of safe integration within the architecture of a system* from [31]

Figure 7 presents a relevant generic vision of sub-systems (i.e. building blocks) integrated in an overall system (e.g. CCS on-board system). All these interactions must be addressed within the OCORA compliant project/program. Figure 8 provides a concrete application of the integrated system under consideration when dealing with OCORA. From Figure 7, it must be understood that

- Maintenance requirement for xx,
- Exported conditions xx for maintenance,
- Operational requirements for xx (refer to [14] for OCORA),
- Exported conditions xx 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 on-board system.

4.2.2 Implementation in OCORA Collaboration

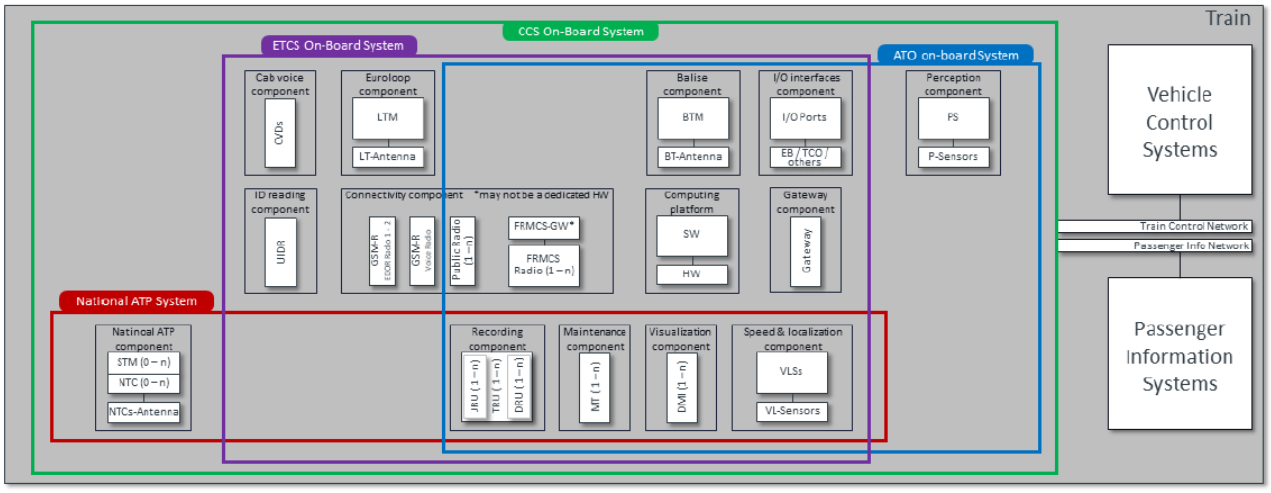

Figure 8 CCS On-board Subsystems Overview

OCORA Collaboration covers topics for the whole CCS on-board system as defined by the TSI CCS [25]. However, as presented on Figure 8, different other systems (i.e. all within the CCS on-board one) exist:

- **National ATP System** refer to Class B systems listed in [32] 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 on-board systems are considered when dealing with integrated safety cases involving OCORA. The same strategy as for the standalone building blocks safety cases will be follow for the integrated safety cases. This means that regarding the whole safety target allocated to the CCS/ETCS on-board system, the use of existing safety data coming from Subset-091 and Subset-088-3 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 realizing a safety case at CCS and/or ETCS level relies on:

- The strategy put in place by the contracting entity (see Figure 9 and Figure 10),
- 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 on-board 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. This is presented in section 5.

4.2.3 Examples of future project architecture

To help the reader to 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 9 and Figure 10 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 on-board 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 realizing the train type safety case.

Key roles

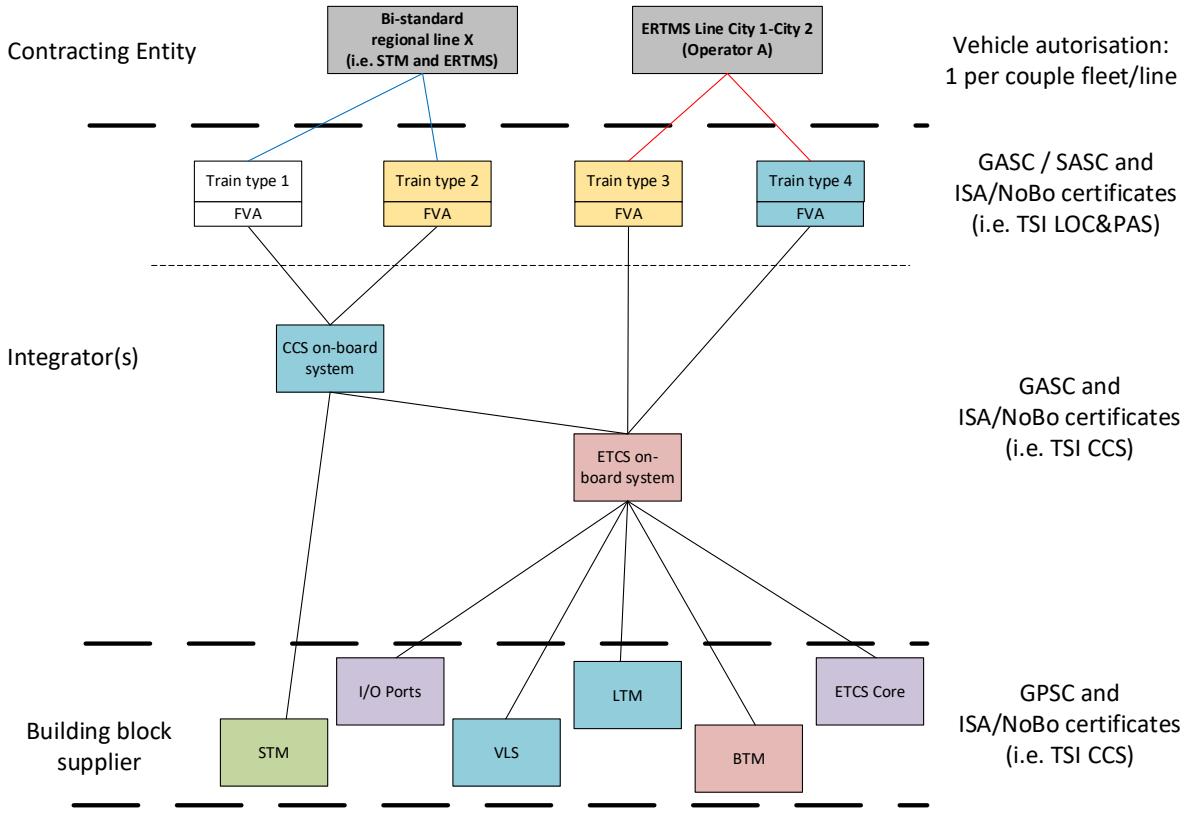

Figure 9 Example 1 of an overall fleet newly defined or retrofitted

Figure 9 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 on-board system for the bi-standard (i.e. both KVB from [32] and ERTMS),

The CCS on-board 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 KVB balises.

Within this architecture, the CCS on-board 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 on-board levels following evolutions. This is exposed in section 5.

Key roles

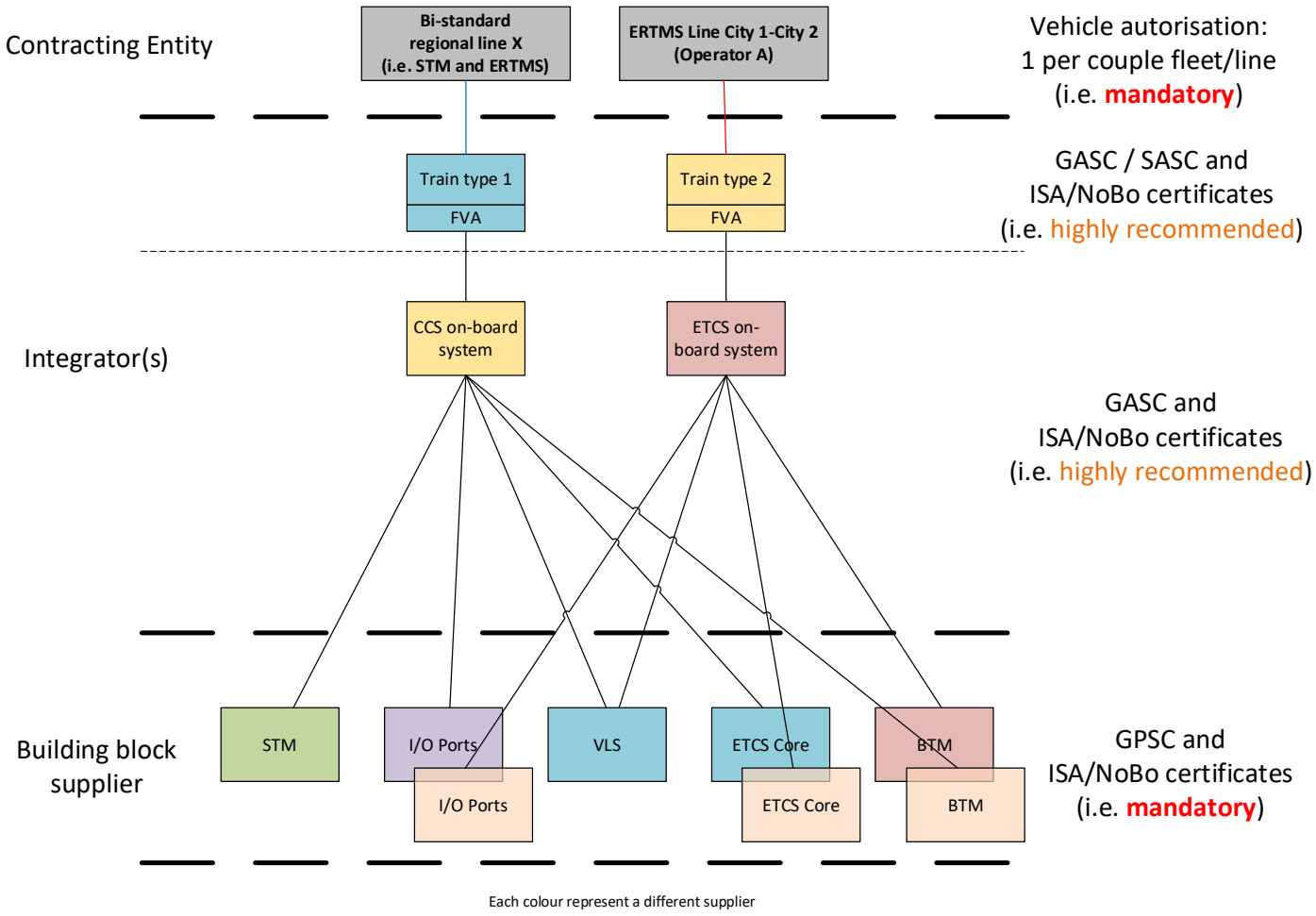

Figure 10 Example 2 of an overall fleet newly defined or retrofitted

Figure 10 presents a different strategy than on Figure 9. 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 9:

- a fleet running on a bi-standard line equipped with a CCS on-board 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 realizing 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 on-board 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.

4.3 SRAC management

4.3.1 Context

This section introduces the way to manage SRAC 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 example provided in Figure 11, based on return of experience from manufacturers and contracting entities, shows the interlinking of SRAC from the ETCS on-board GPSC to the vehicle authorization (i.e. SASC).

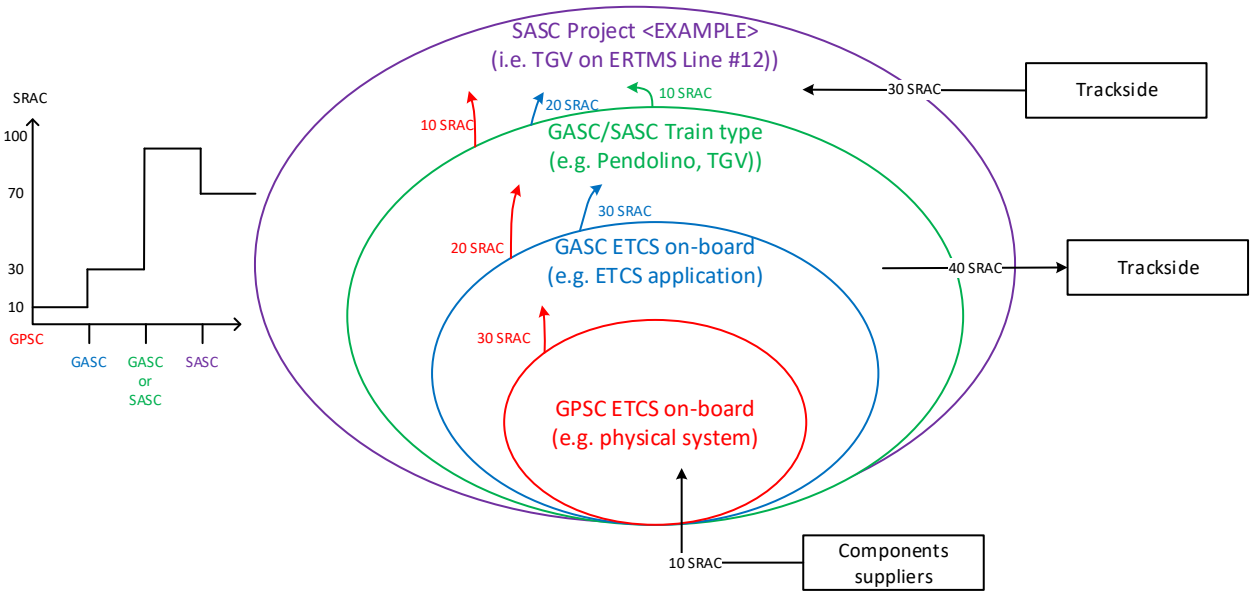

Figure 11 Example of SRAC management of a complete project

The SRAC flows presented in Figure 11 are addressed as follow:

- 10 SRAC coming from safety components used in the ETCS physical system (e.g. FPGA, microcontroller),
- 30 incoming SRAC from ETCS physical system to ETCS on-board application (i.e. red circle on Figure 11),
- Train type GASC inherits 50 SRAC from, both, GPSC (i.e. SRAC not coverable by the ETCS application) and GASC ETCS on-board. In addition, the train exports 40 SRAC to the trackside (e.g. RBC, interlocking) (i.e. green circle on Figure 11),
- Finally, the final safety case, at vehicle authorisation process (i.e. purple circle on Figure 11), shall cover 40 SRAC coming from vehicle side (i.e. GASCs and GPSC) plus 30 SRAC coming from the trackside (e.g. RBC).

Although the figures are not directly coming from existing safety case, the SRAC numbers used are in the range of current deployed projects.

As presented above, 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 uses to induce troubles when covering this kind of SRAC. Because of the important number of SRAC, their coverage requires a lot of time and resources in engineering but for the final vehicle authorization 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.

Within this context, OCORA Collaboration has decided to tackle this topic.

4.3.2 Purpose

Although rules already exist inside EN 50129 [22] 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 presented below (extracted from [4]). In another way, OCORA architecture needs several requirements to help at simplifying the SRAC handling. This is presented in the SRAC management guideline (will be ready in Release 1.0).

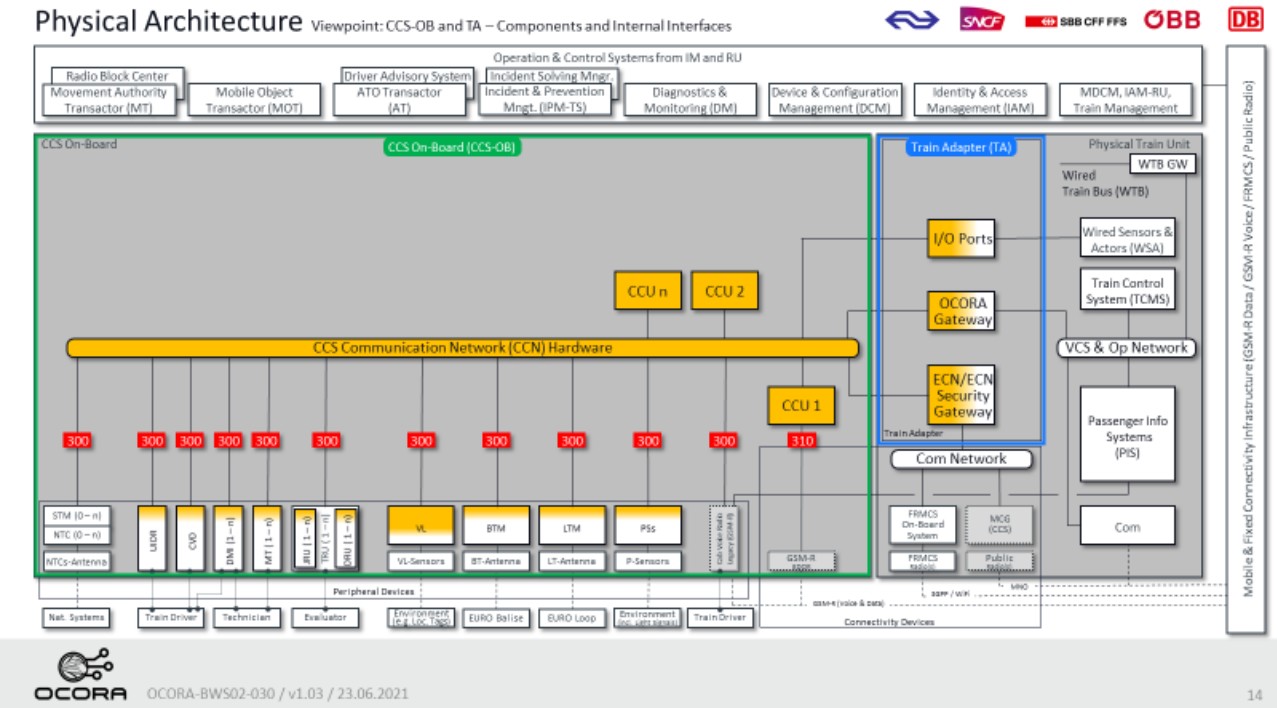

Figure 12 Physical architecture in OCORA Delta release

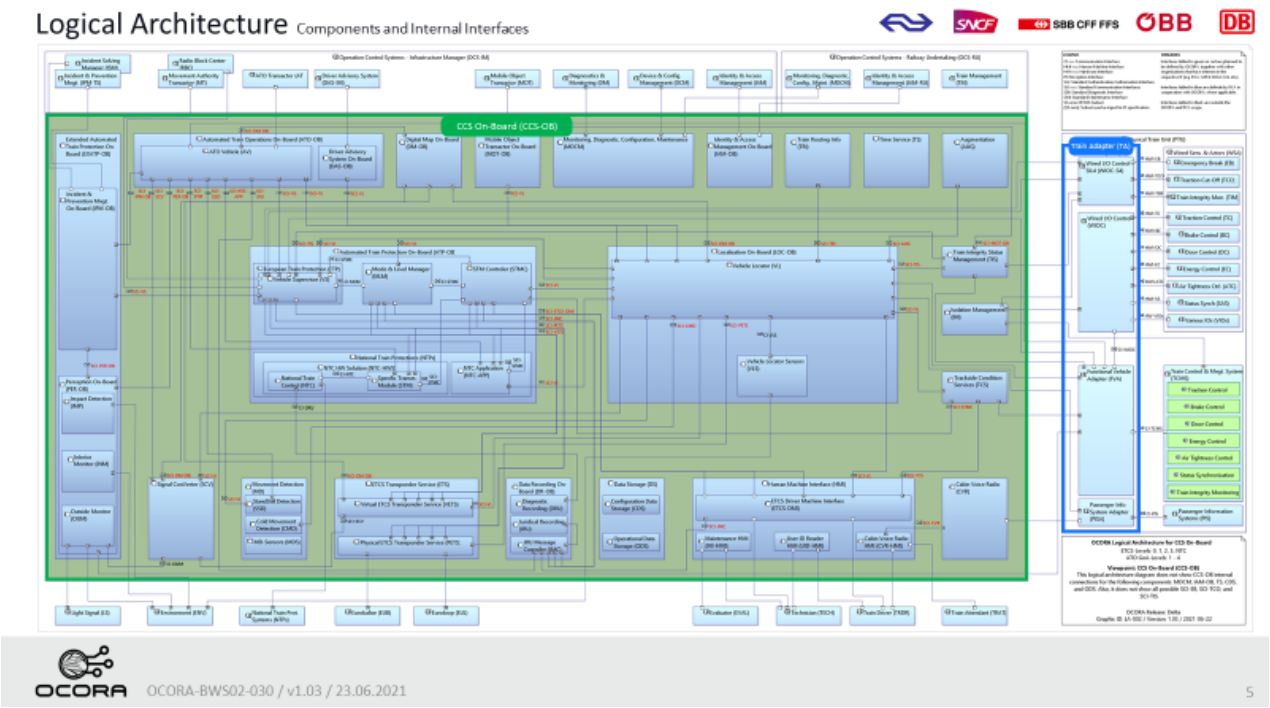

Figure 13 Logical architecture in OCORA Gamma release

The standard interfaces (i.e. red ones in the figure above) issued from OCORA will implicitly result in a set of standardized SRAC at the borders of the building blocks that shall be used by any vendor or integrator dealing with OCORA in its CCS/ETCS on-board system.

Unfortunately, today, it is impossible to ensure that 100% of SRAC at interfaces level will be standardized. Furthermore, additional proprietary SRAC may be emitted for topics not fully handled by OCORA (e.g. operational or maintenance scenario). This must be analyzed during the realization of the SRAC management guideline (will be ready in Release 1.0)in the delta+1 release.

5 Evolutions management

5.1 Context

Evolution management represents a large scope of activities that occurs during the whole CCS/ETCS on-board 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 evolutions in a monolithic system.

For that purpose, the evolution management use to represent an important source of expenses for the operators owning monolithic on-board system.

5.2 Purpose

Based on this previous statement, OCORA Collaboration tends to define an evolution management process (will be ready in Release 1.0) to be deployed by any OCORA compliant project/program. This should help all railway actors involve in the CCS/ETCS on-board system definition to have an easier and cheaper way to handle evolutions during its lifetime.

This process aims at defining the strategy for managing the evolutions of an OCORA compliant CCS/ETCS on-board system once a first assessment has been successfully performed. The evolutions may impact hardware, software, data preparation of the CCS/ETCS on-board system. This documentation aims at providing deterministic results to get a generic and simple common strategy on the way to manage evolutions.

The benefits for the user would:

- a systematic approach possible thanks to the genericity of the OCORA modular architecture,
- faster impact analyses (i.e. design, testing and safety) with a bottom-up approach,
- faster risk assessments following CSM-RA [30],
- faster AsBo assessments because of deployment of a standard and widely use of an approved evolution management process (will be ready in Release 1.0) provided by OCORA Collaboration,
- Cost saving without degrading safety because of rationalization of the overall change management process at project/program level.

6 Assessment management

6.1 Context

OCORA compliant elements (e.g. CCS on-board, building blocks) shall be defined according to TSI CCS [16] which statuses in section 4.2.1.1:

The Control-Command and Signalling On-board and Trackside subsystems shall respect the requirements for ETCS equipment and installations stated in this TSI.

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.

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 Control-Command and Signalling On-board subsystems, the safety level for the service is met.

[…]

Table A 3

List of mandatory standards

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

Note 1: this standard is harmonised, see Commission communication in the framework of the implementation of the Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (OJ C 345, 26.11.2013, p. 3), where also published editorial corrigenda are indicated.

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

- ISA for CENELEC standards (i.e. A1 to A4) or/and AsBo for CSM-RA [30] (in case of significant modifications), 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 for TSI accreditation (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 in case specific NTR (available on ERA's website) applied to the system under consideration (e.g. STM, ETCS application customization for a dedicated country).

All of this constitutes mandatory documentation for ERTMS interoperable systems.

6.2 Purpose

Beside the TSI certification, OCORA compliant systems 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 integrator also needs to be sure that the systems he is buying are ready for a safe integration. Without this, the overall concept of modularity, exchangeability and scalability would not be efficient.

6.2.1 OCORA compliant projects/programs certification

OCORA Collaboration tends to stick as close as possible to what is already available in the current official documentation and directive.

Based on this, the most relevant strategy to handle the "OCORA certification" is to get inspiration from the NoBo certification currently used by all interoperable systems. However, it seems realistic 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 of a mandatory regulation as today for interoperable systems. Knowing this, OCORA Collaboration proposes that the certification will be done through a parallel channel independent of the NoBo one, without a mandatory regulation behind (refer to Figure 14).

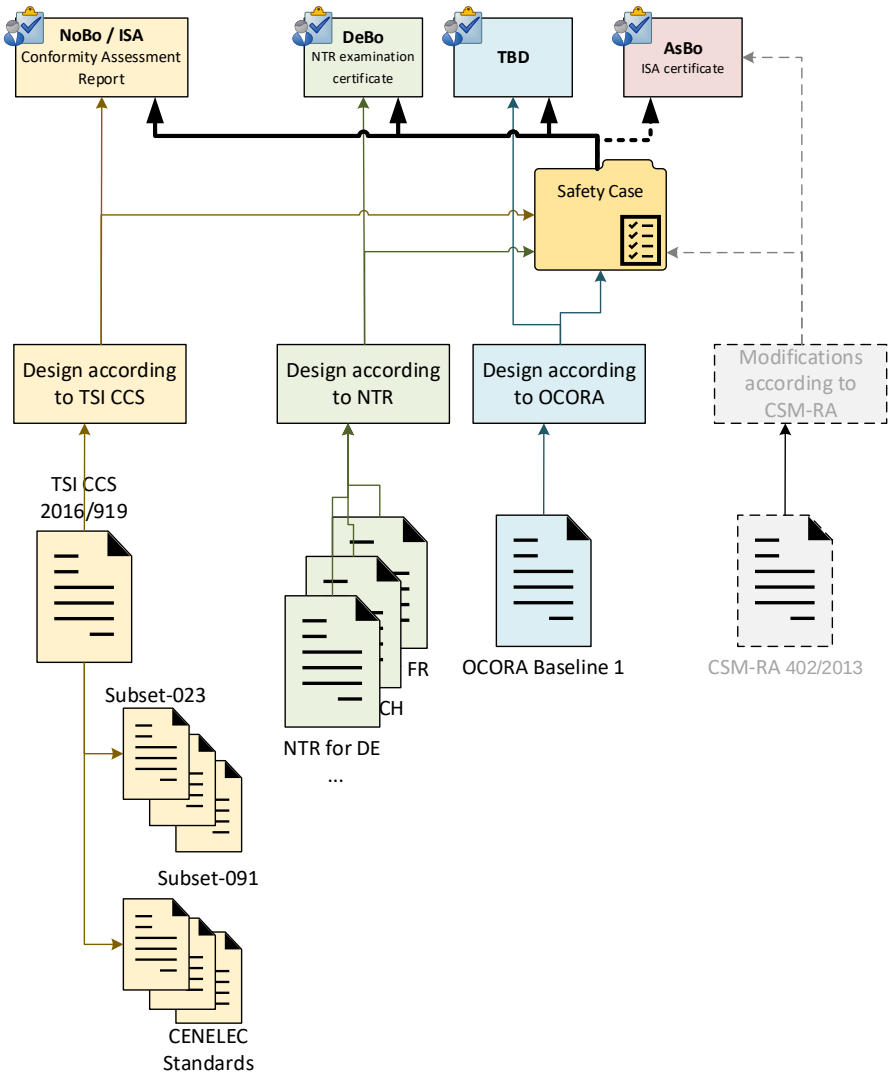

Figure 14 Regulation impacting OCORA compliant systems

The proposition is to define OCORA documentation the same way as the TSI CCS application guide is built [29]. This means that OCORA documentation for procurement will be organized as an application guide (will be ready in Release 1.0) 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 [15]),
- Any release document managed outside of OCORA that is neither called in the TSI CCS [25] or its application guide [29] but mandatory for OCORA deployment (e.g. RCA, Shift2Rail documents).

The complete documentation architecture requested through the different assessment types is presented on Figure 15. A dashed link is proposed between the TSI CCS [25] 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 need to get this “OCORA examination report”. This will be a mandatory request during the call for tender from the contracting entity.

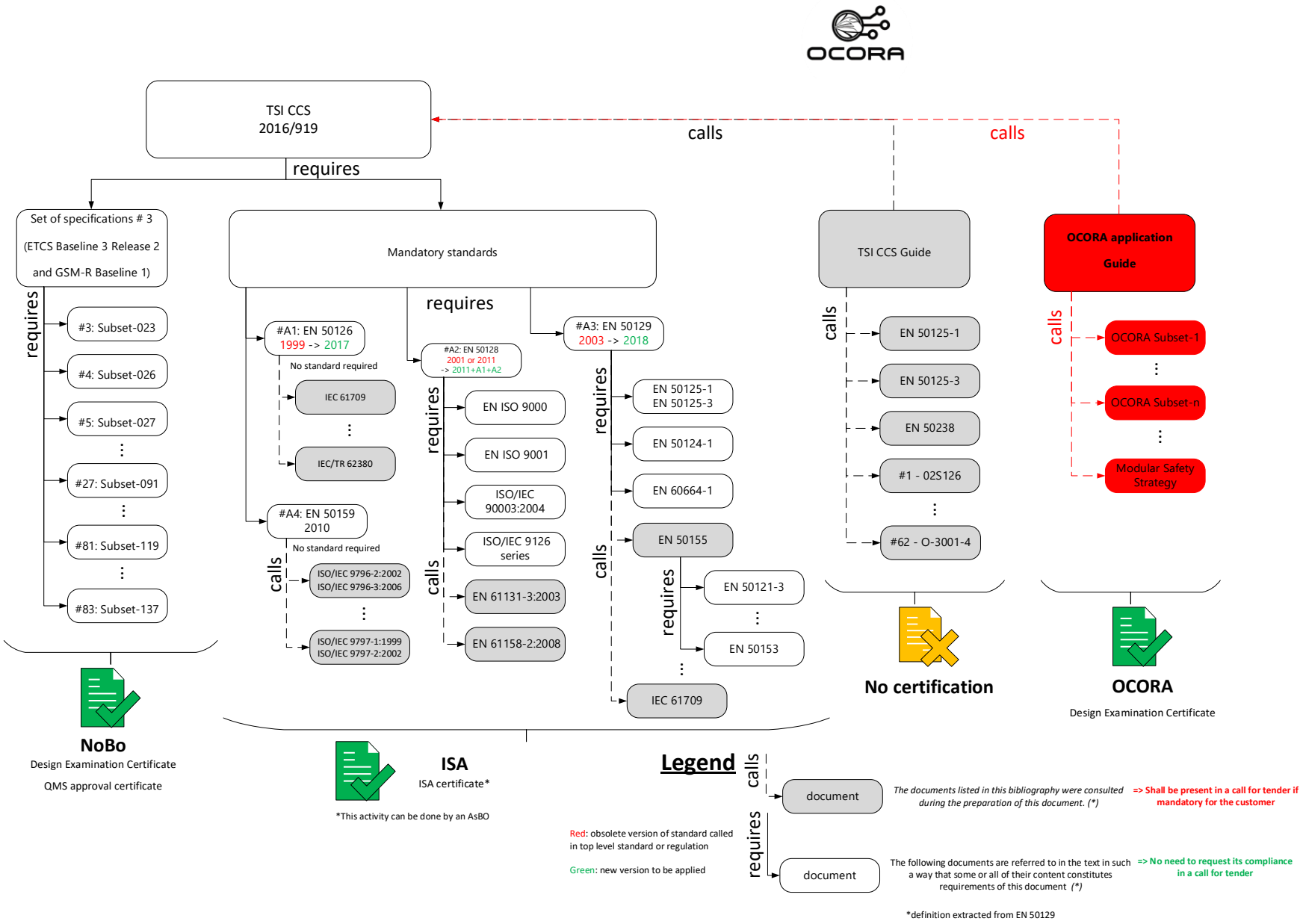

Figure 15 Integration of OCORA certification inside the TSI CCS frame

6.2.2 Cross acceptance

Within OCORA Collaboration, two different kind of cross acceptance are to be considered. The first one is related to the cross-acceptance of already certified products from 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 EN 50506-1 [24] 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 organization 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, an 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 release of OCORA in the cross-acceptance strategy (will be ready in Release 1.0)