OCORA

Open CCS On-board Reference Architecture

Modular Safety
Gamma Release

Document ID: OCORA-40-012-Gamma

Version: 1.01

Date: 04.12.2020

Status: Final

Revision history

Version	Change Description	Name (Initials)	Date of change
0.01	Initial draft, based on RCA_OCORA_WhitePaper_ComputingPlatform_2020-05-26	JB (SBB)	2020-10-12
0.02	Updated following MMo and RMe feedbacks	JB (SBB)	2020-11-02
0.03	Updated to consolidate introduction section (i.e. 2 and 4)	JB (SBB)	2020-11-09
0.04	Update following RMu (SBB), RHe (DB), JBS (SNCF), DSn (NSR) feedbacks Update to cover OCORA Gamma	JB (SBB)	2020-11-19
0.05	Update following SJa (DB), JHo (NSR), SSc (SBB), CGh (SBB) feedbacks	JB (SBB)	2020-11-23
0.06	Update following JHo (NSR), MMo (DB) feedbacks	JB (SBB)	2020-11-24
1.00	All review feedback incorporated	JB (SBB)	2020-11-26
1.01	Minor update to correct typo errors. Final release for Gamma	JB (SBB)	2020-12-04

Table of contents

Table of figures

Table of tables

No table

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.

The following references are used in this document:

[1] OCORA-10-001-Gamma – Release Notes

[2] OCORA-10-003-Gamma – Feedback Form

[3] OCORA-20-003-Gamma – Technical Slide Deck

[4] OCORA-30-001-Gamma – Introduction to OCORA

[5] OCORA-30-002-Gamma – Problem Statements

[6] OCORA-30-010-Gamma – Set of Requirements

[7] OCORA-90-002-Gamma – Glossary

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

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

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

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

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

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

[14] 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

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

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

1 Introduction

1.1 Document context and purpose

This document is published as part of the OCORA Gamma release, together with the documents listed in the release notes [1]. This is the final version of this document for OCORA Gamma release.

This whitepaper should serve as basis for a discussion on a modular safety concept as part of OCORA. It shall give a comprehensive introduction on the need, the principal concepts for realization and the expected benefits as well as issues to be sort out.

This document involves people from different organisations with safety background at different levels (e.g. product, system, project) to address the topics and concerns to get a global vision.

The aim of this document is to identify and implement safety precautions inside the modular architecture presented by OCORA Gamma release. The following high-level questions will be developed:

- Why modular safety?
- Actors that will benefit from modular safety
- What and how modular safety elements shall be addressed?
- Problems with Safety Management in current projects
- Migration strategy

This document does not attempt to provide solutions to all issues highlighted. Their development will be scheduled from next year and will require, in addition of the OCORA working group, external actors support from industry (e.g. suppliers, assessors, international organisations) to consolidate the management of modular safety.

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

This document is addressed to safety managers 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 Gamma 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 [4], the Problem Statements [5] and the Requirements [6]. The reader should also be aware of the Glossary [7].

1.3 Definition and acronyms

Refer to OCORA glossary [7] for the definition of acronyms.

2 Why modular safety?

Why do we need Modular Safety for OCORA and what is its purpose? There is a simple answer to this:

Safety is a mandatory requirement for CCS solutions. Without mastering modular safety, modularity, upgradeability and interchangeability can't be reached for the OCORA system. So, it is a clear enabler for OCORA.

Without Modular Safety, i.e. handling the Safety Management as today, we will not be able to manage the evolution of system in most of its areas and there will be no real cost savings. So, it must be stated, that the existing standards and methods limit evolution of CCS systems over their lifetime.

The monolithic approach for CCS onboard systems makes changes of individual modules almost impossible without impacting the complete system. As a result, the complete system needs to be reassessed (i.e. effort). The project specific safety management and lack of modular thinking result in complex nesting of SRACs and adds unwanted complexity. In total, the cost for managing the safety is extremely high (especially compared to the development effort) and there is little reuse possible.

It is essential for OCORA to adapt Safety Management to the modular approach to fulfil the mission goals (see [5]).

3 Actors that will benefit from modular safety

From a general point of view, this modular approach will stimulate the railway market by allowing new players who can provide one or several building blocks without dealing with the complete CCS on-board systems. This will increase technical innovation and competition between the vendors and decrease the overall price of the systems.

A modular architecture and thus a modular safety approach could bring benefits to a large part of the stakeholders involved in the realization of CCS on-board systems:

- Industry's suppliers:

  A modular safety approach will bring to them much more flexibility for managing modifications on their solutions without necessary impacting the assessment of the whole system at specific application level. The modifications concern (not exhaustive):

  - Hardware parts: more freedom on the obsolescence management of components, especially the non-safety related ones. More freedom to perform improvements (e.g. electromagnetic interferences protection, mechanical modification(s) to ease maintenance activities, manufacturing processing of boards),
  - Software parts: more freedom to perform preventive or corrective maintenance (i.e. bugs), especially related to non-safety elements. More freedom to add new non-safety functionalities.

  The modification of safety related items should also be simplified and thus become less expensive thanks to the generic safety methodology for modifications handling defined by this working group.

- Integrators:

  A modular safety approach, as presented on Figure 2 will provide flexibility to the integrators when building their CCS on-board system. Indeed, exchanges or addition of building blocks (e.g. from other vendors) will be eased for:

  - integration: the OCORA modular architecture will provide specified boundaries between the building blocks. Thus, the integration of the building blocks together, used as "black boxes" will ease the validation process,
  - assessment: the scope will be on the integration of the modules together, based on cross-acceptance of the building blocks. In addition, the improved management of SRAC proposed by this working group should decrease the complexity of the overall safety demonstration.

- Railway undertakings:

  A modular safety approach will allow a much easier evolution of the CCS on-board system than today. Indeed, thanks to modular safety, addition of functionalities will be cheaper and implemented quicker than today thanks to the improvement of the assessment process.

  This modularity will also avoid vendor lock-in situations caused by the monolithic architecture. The railway undertakings can build their own CCS on-board system based on independent building blocks provided by different suppliers and can get spare parts from different vendors to improve the lifecycle process.

- Assessors:

  The decomposition of the monolithic block into smaller parts will ease the assessment activities by providing simplified systems with fewer safety requirements (including SRAC) and clearer interfaces than today. Furthermore, the homogeneity of the safety analyses in case of modifications (i.e. thanks to the generic strategy defined) will help the assessor to focus on the key elements modified and on non-regression activities.

  The clarification of the responsibilities within the CCS on-board system will also simplify the tasks of the assessors, especially when dealing at specific project level. Indeed, they use to hold the responsibility (i.e. from a juridical point of view) for the whole system whereas its assessment is only focusing on the

specific application. The new cross-acceptance strategy should balance the responsibilities between the different assessment levels.

4 What and how modular safety elements shall be addressed?

These key elements will be addressed and scheduled in a dedicated separated document (out of scope of the whitepaper).

- OCORA modular architecture:

  The OCORA Gamma Architecture (Figure 1) shall respect the needs of Modular Safety and vice versa. A generic safety analyse will be performed and a working methodology for the various design activities will be developed to integrate modular safety in the further detailing of the OCORA architecture.

  Modular Safety will provide safety elements (e.g. hazard, THR) required to reach independence for the building blocks. Independence means that any building block shall be certified as stand-alone equipments without requesting an overall assessment of the CCS on-board system.

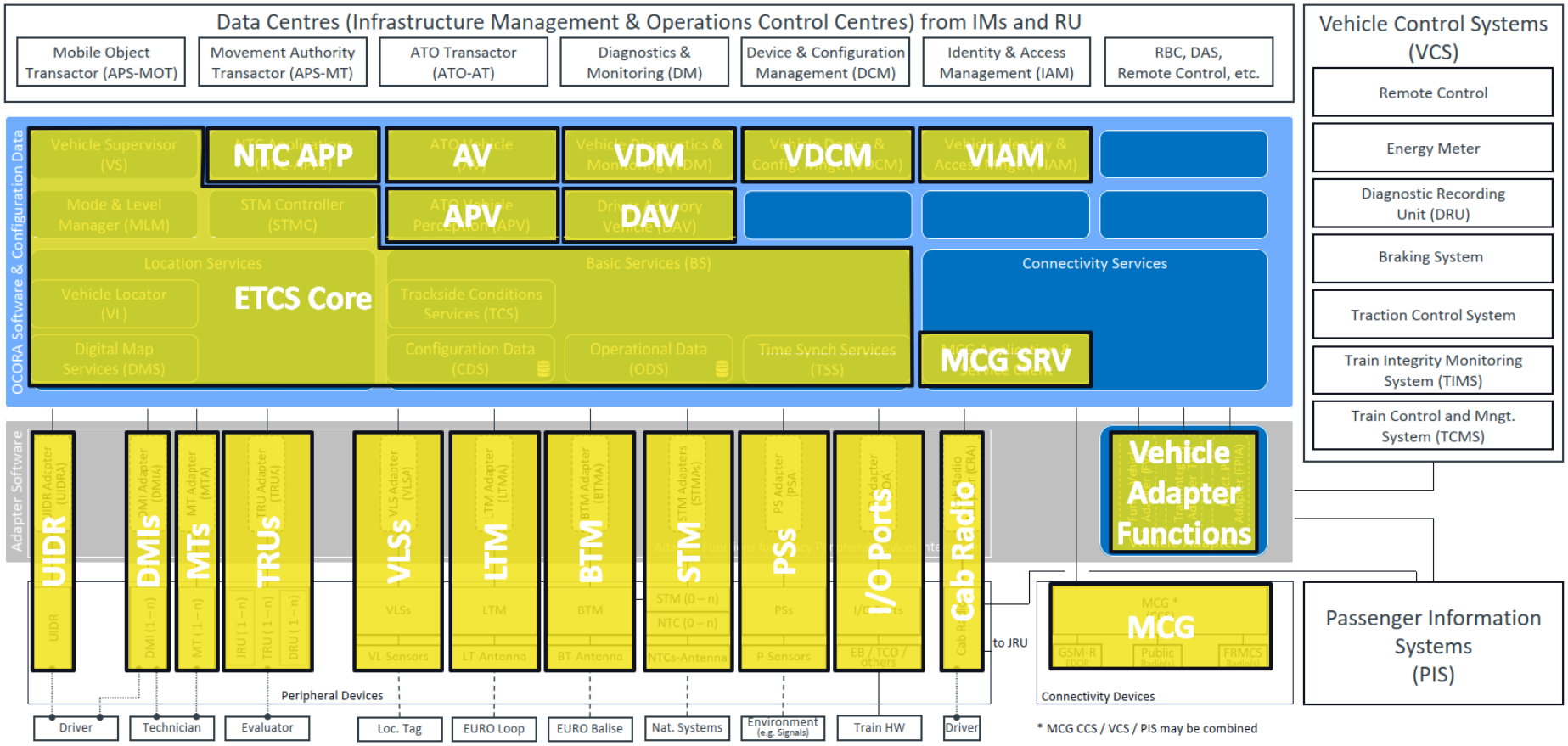

Figure 1. Functional building blocks from OCORA Gamma release [3]

- Safety Cases nesting:

  As presented in section 5, the safety cases management including the SRAC can be very difficult for vendors and integrators. A strategy related to their nesting based on modular safety shall be defined. An overview is proposed on Figure 2. This strategy shall also manage the SRAC topic to improve their management at the different safety case levels (e.g. standardisation, simplification and limited number of SRAC).

  Two sub-topics can be addressed:

  - Safety case nesting: planned for the OCORA Delta release, the safety cases that shall be processed in an OCORA environment must be defined. This includes the hierarchy (e.g. GPSC, GASC, SASC), responsibilities and scope for each of them,

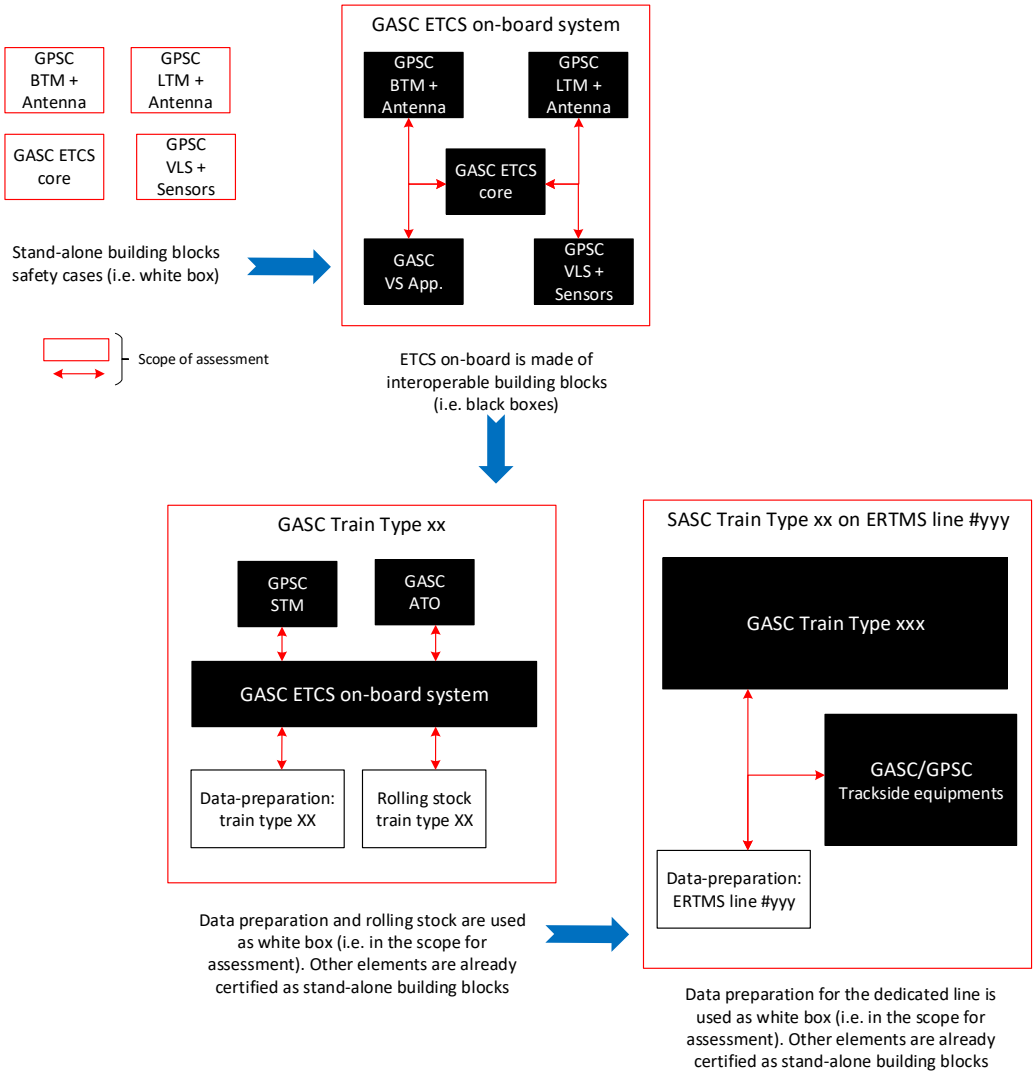

Figure 2. Overview of imbrication of modular safety cases

  - SRAC management towards OCORA: this topic should be based on experience feedback about the reasons of the complexity of the SRAC management at all safety case levels. Following that, means and methods to improve this workflow shall be defined. A method should propose a clear acceptance process for defining SRAC.

- Review of the TSI CCS to be aligned with a modular approach:

  Safety requirements including hazards and their associated TFFR are summarised in SUBSET-091 for interoperable components. Unfortunately, the latter only covers ERTMS Level 1 and Level 2 and obviously, is not yet in line with OCORA architecture as it presents the ETCS on-board system as a monolithic block (refer to Figure 3). A deep analysis of the TSI SUBSET related to safety (i.e. 088, 091, 120) shall be performed to identify all the required changes to be applied to support modular safety.

A strategy for the TSI CCS evolution needs to be defined.

- Reinforce cross-acceptance between assessors:

  It is a fact that today, the cross-acceptance of certified building blocks may be challenged at upper level by a different assessor and thus induces a high impact on costs and planning at GASC or SASC levels. This must be avoided to keep the benefits of a modular architecture deployment. One problematic point relies on the limit of responsibility between the different safety cases (i.e. GPSC -> GASC) when submitted to cross-acceptance. Indeed, EN 50506-1 [13] does not assign responsibilities when products or systems are used in a cross-acceptance process.

  To get an efficient modular safety concept, this group shall propose an assessment strategy in line with EN 50506-1 [13] to ease the cross-acceptance concept. One of the goals should be the definition of responsibilities at different integration levels for an overall system based on stand-alone building blocks. Another goal will be to define the keys elements related to OCORA (e.g. interfaces compliance) that should be mandatory in the assessment report. This should avoid the building blocks certificates to be challenged at higher-level (GASC or SASC). Another goal will be to define the key elements related to OCORA (e.g. interfaces compliance) that should be mandatory in the assessment report. This should avoid the building blocks certificates to be challenged at higher-level (GASC or SASC).

- Strategy to manage CCS on-board system evolutions:

  As presented in section 2, some high costs related to the CCS on-board systems concern their assessments when modifications occur. The definition of a modular architecture will help at improving this topic. CSM-RA [15] already oversees the modification management for safety related systems but it can be improved while introducing a modular architecture approach. In addition, this group shall propose a panel of assessment levels depending of the modification impact. This could start from a yearly letter of support (i.e. minor non-safety related evolutions) to a new certificate when safety elements are modified.

- Testing activities related to a modular architecture:

  A large part of the evidences used in the safety cases to validate the safety requirements relies on the correct execution of tests. Testing ensures that the functional and non-functional (for most of them) specifications are correctly implemented in the building block, including its external interfaces. This needs to be addressed in relation to the OCORA Technical Workstreams testing and acceptance of global standards.

5 Problems with Safety Management in current projects

To illustrate the limitation of evolutions for the CCS on-board systems, the following problems of the today non-modular solutions have been highlighted. They need to be resolved by the modular safety approach and act as problem statement.

- Assessment costs are too expensive:

  Safety is a crucial element of CCS functionality. Proving it causes serious effort and costs at program or project level. Today's assessment (i.e. CENELEC standards [8] to [13] and NoBo [14]) is based on the monolithic block system defined on Figure 3. This leads to deploy important means for safety demonstration for the first time and again in case modifications in the CCS on-board system. Indeed, impact analyses, especially at low level hardware or software are complicated. This difficulty is highlighted on Figure 4 with the supplier's proper boundary (dashed line) as, depending where the modification(s) occur, he may have an unexpected impact on both the ETCS application and the low level software when only one part is modified.

  This collateral effect has a direct negative impact on V&V and assessment amount of activities, costs and planning.

- Monolithic approach for CCS on-board systems:

  In today's version of TSI CCS, the ETCS on-board system, which corresponds to the largest part of the CCS on-board system (e.g. ETCS plus management of national systems), is defined as a monolithic block in SUBSET-026 as presented below:

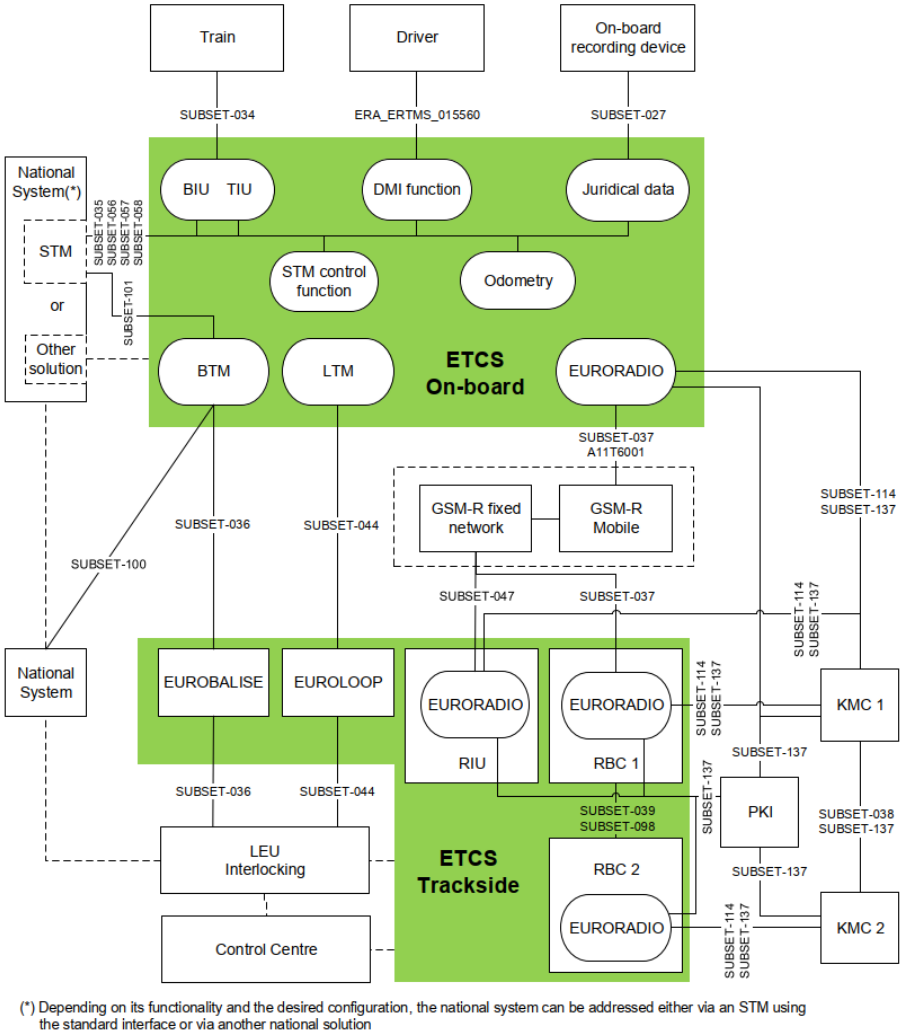

Figure 3. ERTMS/ETCS system and its interfaces according to TSI CCS SUBSET-026-2)

This system's definition deals with a large and complex box where no clear borders are defined. The separation of the monolithic system into smaller building blocks (e.g. BTM, LTM) is not standardized and is defined with proprietary interfaces. Because of this, it is almost impossible to modify one of them without impacting the whole CCS on-board system. The impact at project level (i.e. specific application) is usually so expensive that the non-mandatory evolutions are withdrawn and thus, the CCS on-board system does not evolve as it is expected over its lifetime.

Another impact of the monolithic block design resulting in the shortage of evolution consists in the lack of standard boundaries between low-level software (e.g. runtime, services, OS, drivers) and ETCS application. Figure 4 presents the theorical functional border (in red) which separates the source code related to pure ETCS behaviour (i.e. as defined in SUBSET-026) and the boundary applied by a supplier (dashed line). The definition of the red line itself is not technically defined by TSI CCS thus it is almost impossible to define a regular boundary between the low-level software and the ETCS functionality.

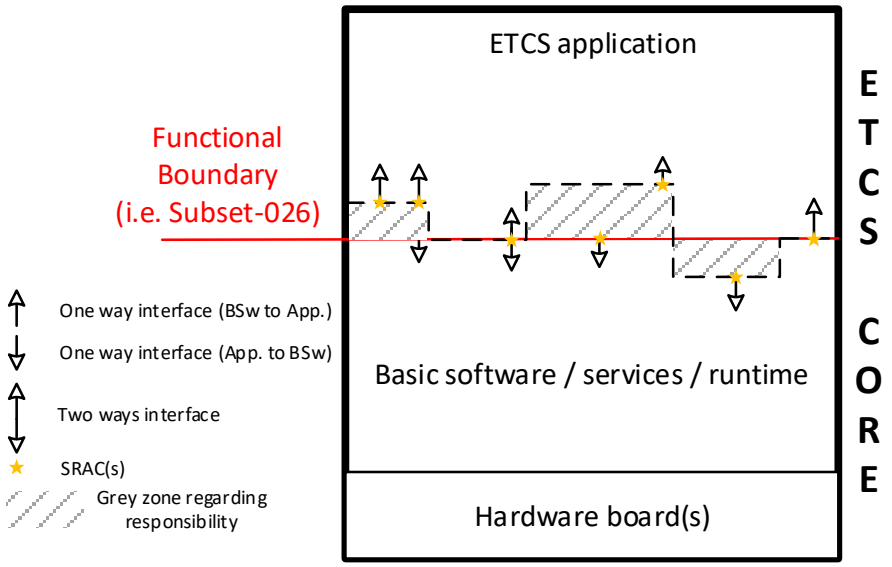

Figure 4. Today's situation regarding non standardized interfaces

- Heaviness of SRAC management throughout system development:

  The lack of standardized interfaces between the building blocks of the CCS on-board system and between ETCS applications to the low level software lead the suppliers to define their own boundaries inside the design where sometimes the limit of responsibilities is not obvious (i.e. refer to the grey zones on Figure 4). When acting this way, the supplier will have to raise a large number of SRACs to upper level safety case(s). These SRAC use to be very complex because of their related interfaces description and are often source of troubles and confusion at application level (i.e. generic or specific). Most of the time, they are not complete or clear enough (e.g. hazardeous event and barriers) to be smoothly covered. In the worst case, they are wrongly covered, and can lead to safety issues.

  An example of SRAC spreading (based on a vendor safety case at train type level) between the different safety cases is recapped hereafter:

  - 55 incoming SRAC from lower-level GPSC and GASC (i.e. red and blue circles on Figure 5),
  - 15 out of scope SRAC (i.e. not applicable for this train type),
  - 23 transferred SRAC to upper level (i.e. not closable at train type level) (i.e. purple circle on Figure 5),

  This represents a total of 93 SRAC.

  Then, this safety case exports also its own 116 SRAC to the other levels:

  - 18 SRAC applicable directly to the customer (e.g. driver rules, maintainer operation),
  - 14 SRAC applicable to the technical system related to the specific application (e.g. rules for parameter ranges, national values, STM management),

- 84 applicable to the trackside (e.g. EUROBALISE data preparation, balise groups linking, national rules for trackside)

The following figure illustrates the complexity of SRAC nesting (figures are just presented as another example):

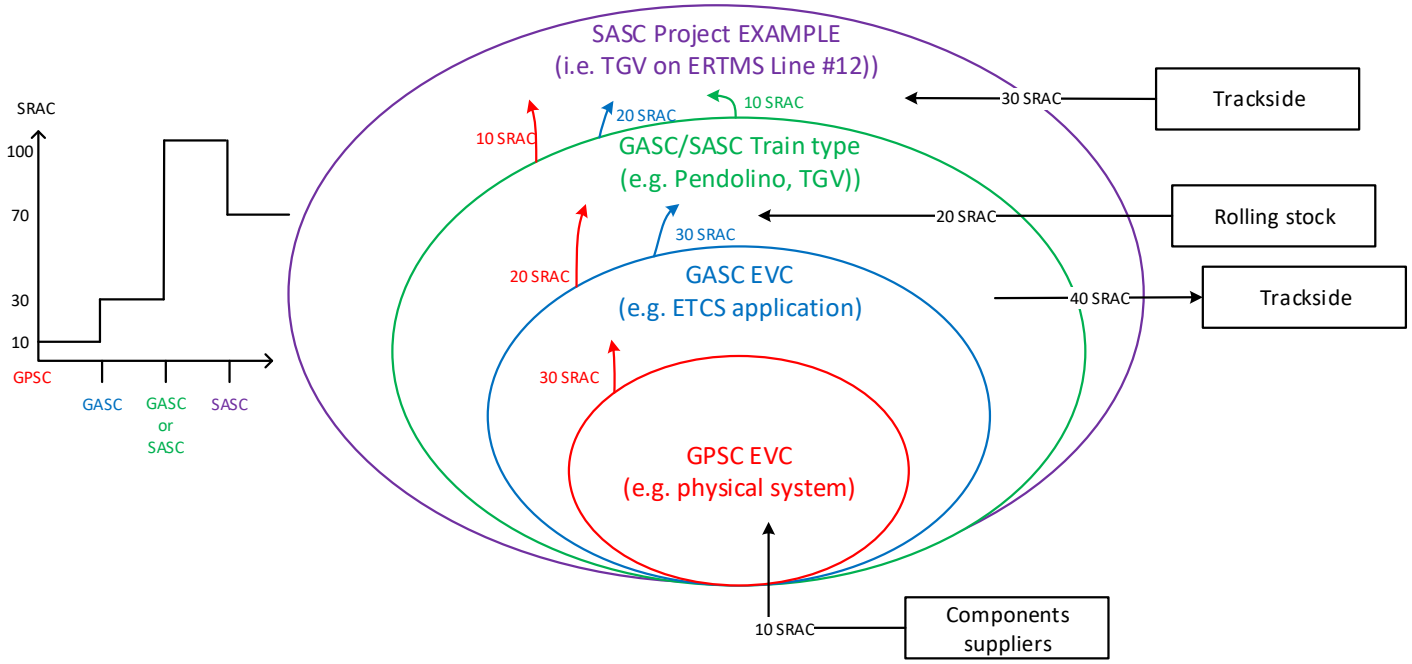

Figure 5. Safety management of SRAC

Managing these non-standardized SRAC at project level implies a larger scope for the hazard log with additional analyses to find the correct coverage. In case a project modifies its CCS on-board system with a different supplier's equipment, the complete SRAC analysis at SASC shall be performed again from scratch and will have an important impact on assessment costs.

6 Migration strategy

Besides the mid-term and long-term benefits of rolling out Modular Safety, it is important to also anticipate the difficulties that will likely raise when deploying it in a short-term period. This will be a reality for the first product release (i.e. building blocks), CCS on-board systems and their assessments. Regarding this, another task to be addressed by the modular safety working group will be to early identify these critical points and try to find solutions in order to minimize their impact. Impacted actors (e.g. vendors, assessor, railway undertakings) can then be involved to integrate these mitigations into their developments.