OCORA

Open CCS On-board Reference Architecture

RAMS – SRAC/AC Management

Document ID: OCORA-TWS07-030

Version: 2.60

Date: 09.06.2022

Revision history

Version	Change Description	Initial	Date of change
1.00	Inherited content from draft “Safety Strategy” version for OCORA Delta Release	PN	01.08.2021
1.01	Definition of the document structure based on the R1 template	PN	03.11.2021
1.02	Update according to member’s review. Complete all section	PN	16.11.2021
1.03	Update according to SRAC and Evolution members reviews	JB	17.11.2021
2.00	Official version for OCORA Release R1	JB	18.11.2021
2.50	Update for OCORA Release R2	PN	30.05.2022
2.60	Official version for OCORA Release	PN	09.06.2022

Table of contents

Table of figures

Table of tables

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.

OCORA-BWS01-010 – Release Notes

OCORA-BWS01-020 – Glossary

OCORA-BWS01-030 – Question and Answers

[1] OCORA-BWS01-040 – Feedback Form

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

[3] OCORA-BWS04-010 – Problem Statements

[4]

[5] OCORA-TWS07-010 – RAMS – Modular Safety Strategy

[6] OCORA-TWS07-020 – RAMS – Evolution Management

[7] OCORA-TWS07-040 – RAMS – Optimized Approval Process

[8]

[9] OCORA-TWS07-050 – RAMS – RAM Strategy

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

[11]

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

1 Introduction

1.1 Purpose of the document

The purpose of this document is to describe the management of safety and non-safety related application conditions (SRACs resp. ACs) within OCORA compliant projects.

SRACs establish the safety-related assumptions and conditions that need to be satisfied to mitigate risks when the system under consideration is integrated. The need for a standardized SRAC/AC management within OCORA compliant programs comes from a common return of experience from railway undertakings. Although rules for SRAC writing already exist inside EN 50129 [12], a process design for SRAC/AC management is still outstanding. The sharing of SRACs/ACs between different levels of safety cases usually induces misunderstandings due to a lack of communication between SRAC/AC emitters and receivers which can, in the worst case, drive to an incorrect coverage and lead to a safety issue.

The correct definition, processing, and handling of SRACs/ACs is essential and a precondition for safe integration. Working with a predefined SRAC/AC management processes is not mandatory, when the current SRAC/AC management process inside the contracting entity (in charge of the overall OCORA compliant project) fully covers its expectations. However, SRAC/AC management is highly recommended and represents one of the key factors for bringing OCORA to success. OCORA provides the opportunity to improve complex SRAC/AC management thanks to its modular architecture. Besides, OCORA architecture needs several requirements to help simplifying the SRAC/AC handling.

This document is structured as follows:

- Pain points of current SRAC application regarding OCORA (chapter 2)
- SRACs/ACs in OCORA (chapter 3)
- SRAC/AC Management within OCORA compliant projects (chapter 4)
- Outlook on further deliverables (chapter 5)

The following deliverables in the context of SRAC/AC management in OCORA compliant projects will be addressed and published in this and the following OCORA releases:

- OCORA AC management guideline *(*i.e. efficient dialogue and exchanges between SRAC/AC emitters up to final SRAC/AC implementers) recommended for all OCORA compliant programs)
- OCORA AC template with strictly defined rules for the documentation of ACs/SRACs (expected to be mandatory for all OCORA compliant programs)
- OCORA Standardized AC list to be deployed on the interaction of different Building Blocks (BB) with the external world. These SRAC/ACs can be standardized because they will rely on fully defined interfaces (OCORA, ERTMS Subsets, CONNECTA and other European initiatives).
- OCORA Non-standardized ACs definition rules for defining a framework in which non-standardized SRACs/ACs are allowed to be defined within OCORA (SRACs must not go against modularity)

Unlike in Release R1 the scope of this whitepaper has been extended from “safety-related application conditions (SRACs)” to SRACs/ACs by adding the more general term “application conditions (ACs)”, as there are ACs not related to safety but strongly related to availability or reliability issues and therefore also have to be taken into account within building block design.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

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

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

1.2 Applicability of the document

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

1.3 Context of the document

This document is published as part of the OCORA Release R2, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

The Whitepaper on SRAC/AC Management is connected to other RAMS deliveries which are also part of the R2 release. Figure 1 presents the link between these different deliverables. It must be noticed that the Whitepapers on SRAC/AC Management, on Evolution Management, on Optimized Approval Process and on RAM Strategy are additional documents besides the documents according to the formal CENELEC V cycle Documentation (represented in brown in the figure below) required for the new modular approach.

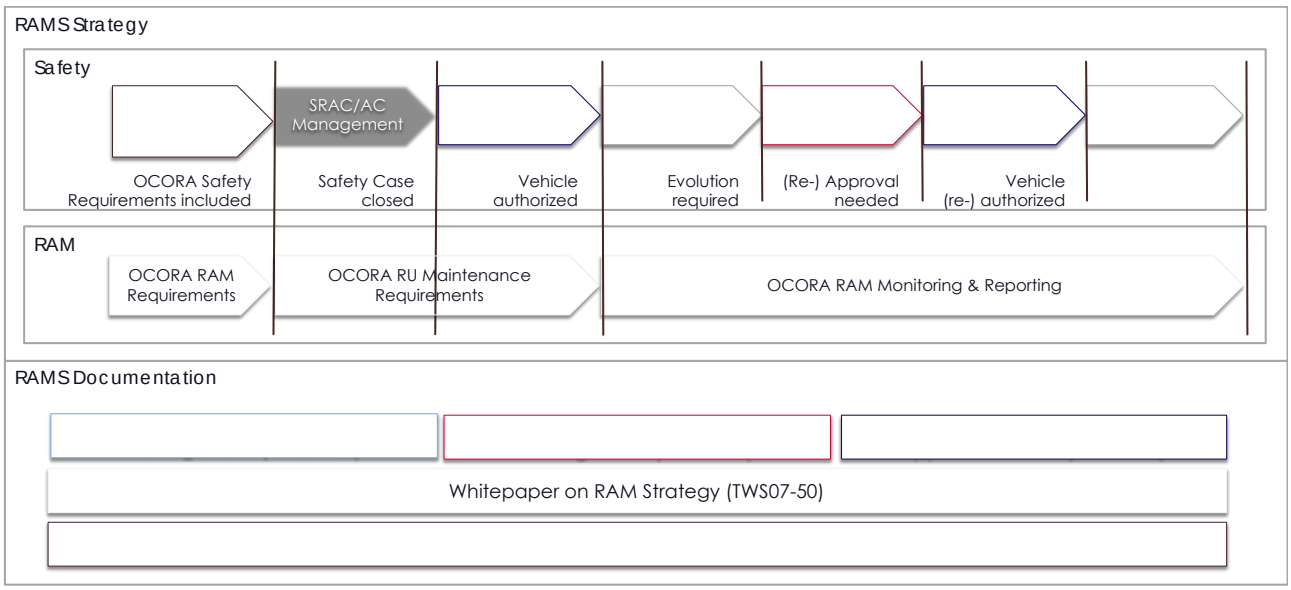

Figure 1 OCORA RAMS Strategy and RAMS Documentation

2 Pain points of current SRAC/AC application regarding OCORA

In this section, existing regulations, process descriptions and templates regarding the current management of SRACs/ACs should be reviewed and compared with experiences from practice. The goal is to identify current pain points as well as missing or misunderstood information regarding current SRAC/AC management, which have to be addressed for SRAC/AC Management within OCORA's modular approach.

2.1 Comparison and analysis of existing SRAC processes

Starting point of the analysis was the CENELEC regulation EN 50129 regarding "Safety related electronic systems for signalling". Here a generic definition of SRAC is given and mandatory recommendations are defined (for example "SRACs shall be uniquely identifiable" or "Avoid declaring SRACs that could have been avoided through design"). Besides an exemplary categorization for SRACs an example for an SRAC template is given. [64]

Identifier	Unique identifier
Title	Short title (useful to promptly recall or sort out the SRAC)
Origin	Indication of originating activity / document
Hazard(s)	Indication of related hazard(s)
Receiver	Indication of phase/entity (e.g. application design, installation, maintenance) receiving the SRAC
Text	Text of the SRAC
Verification	Examples of how it might be possible to comply with the SRAC (test, inspection, specific documentation). Examples based on past projects experience can be given where/when available

Figure 2 SRAC template example presented in EN 50129

As the SRAC information provided by the EN 50129 are presented in a high-level and generic way, several RU have their own guidelines and templates for handling with SRACs, which must be analysed in the context of this whitepaper. Up to now, the following input documents have been used for recording the status quo of SRAC management besides the CENELC standard EN 50129 input documents from DB, NS, SBB and SNCF have been analysed.

For comparing the SRAC information given by the EN 50129 and the specific guidelines of the RU, the information was grouped in the five categories presented in Table 1. The categories represent information regarding the Definition of SRACs, requirements/recommendations for correct SRAC application, involved roles and responsibilities as well as process descriptions, process flow charts or other templates regarding the definition or handling of SRACs.

Definition of SRACs	Requirements for SRAC application	Roles and responsibilities	SRAC processes	Templates

Table 1 Categorization of SRAC information contained in the reviewed documents

The results of the first analysis is shown in the figures in the previous version of this document. In the next steps the main content has to be consolidated and translated into recommendations and requirements for the handling with SRACs/ACs (ref. 3.3). An SRAC/AC process flow chart for non-standardized SRACs/ACs is generated where the process between SRAC/AC emission to its final coverage with different steps can be defined in the context of OCORA.

2.2 Identification of pain points for OCORA's modular approach

Main pain points of current SRAC management processes identified by OCORA team members:

- The SRAC doesn't cover the lifetime of a system, e.g. a project modifies a part of the system which is covered by a SRAC but the project is no more aware of that, as the SRAC had been emitted at the very beginning of the project and its coverage has been slightly modified release after release of documentation and so the latest coverage does not fit anymore and activities with critical safety impact are done by the project.
- Lack of interaction between SRAC emitters and receivers
- Insufficient definition of the SRAC context (required by EN 50129 but not sufficiently challenged by ISA)
- Lack of examples for mechanisms to be deployed to cover the SRAC
- System hazards for SRACs not clearly identified (required by EN 50129 but not sufficiently challenged by ISA)
- Misunderstandings while sharing SRAC between different levels of safety cases, which can, in the worst case, drive to an incorrect coverage and lead to a safety issue.
- Absence of a standardized format for SRACs; each project / supplier / RU uses his own format
- No justification of the SRAC; in some cases, RU have to implement SRAC (e.g. for maintenance) without being aware of the expected coverage or the its frequency of realisation.

The last point is related to a general challenge regarding the inheritance and interlinking of SRACs from the ETCS on-board GPSC to the vehicle authorization (i.e. SASC). The example provided in Figure 3 is based on return of experience from manufacturers and contracting entities.

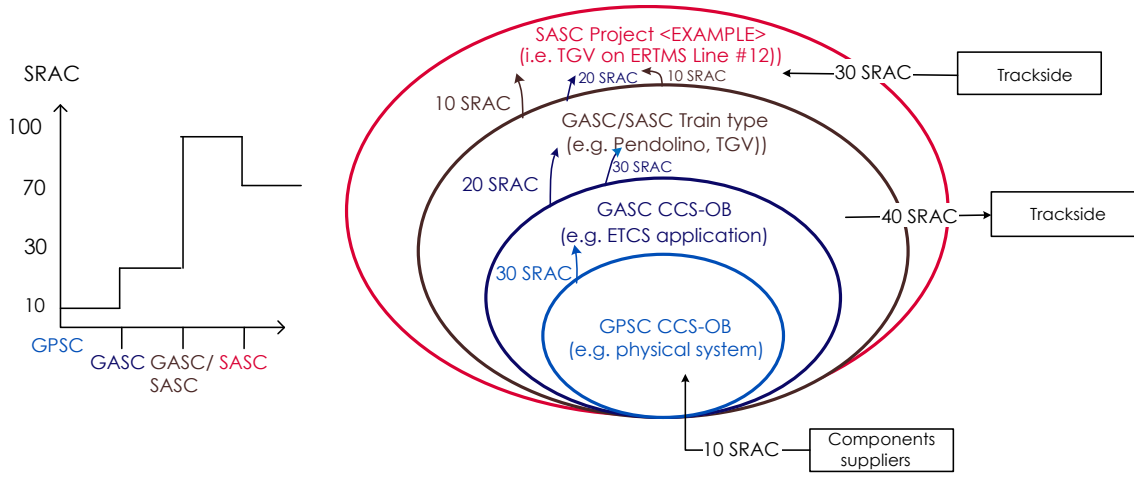

Figure 3 Inheritance of SRACs during integration processes

The SRAC flows presented in Figure 3 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 2),
- 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 authorization process shall cover **40 SRAC**

As presented above, the highest level of safety case uses to deal with very low level SRAC coming from the 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 high number of SRACs, their coverage requires a lot of time and resources in engineering and 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. The example provided in Figure 3 is based on existing safety cases from manufacturers and contracting entities, shows the interlinking of SRAC from the ETCS on-board GPSC to the vehicle authorization (i.e. SASC).

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.

3 Understanding of SRACs/ACs in OCORA

3.1 Definition of SRACs

Resulting from the analysis of the SRAC processes of EN 50129 [12] and the RU's management guidelines in 2, an SRAC in OCORA compliant project is defined as follows:

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. For closing the SuC's safety case when it is integrated in an overall system, the SRACs need to be fulfilled by a receiving entity

The risk owner, the emitting entity (EE) of the SRAC, specifies the requirements for the control measures in order to mitigate the risk on the side of the receiving entity (RE). After there is a common understanding about the SRAC and the way of coverage, the RE is responsible for mitigating the risk. The OCORA SRAC management process with the help of a standardized OCORA SRAC template is described in 4.

Already recognizable 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.

3.2 Standardized SRACs and safety requirements

In the OCORA context SRACs/ACs can be seen as constraints and application rules exported from the OCORA building blocks (BB). According to OCORA's goal to standardize the CCS-OB architecture, all the BB inside the CCS-OB should be standardized and should be connected via standardized interfaces. In this case also the safety requirements for the BB are based on the overall CCS-OB hazard analysis and defined. Because of standardized BB and defined safety requirements, at a final stage, there will be no need for emitting SRACs from one BB to another or (as currently often implemented) bottom-up from one BB to the integration level within CCS-OB. The constraints and application rules will be defined top-down through OCORA's CCS-OB design and directly become safety requirements. SRACs will be only needed for interfaces outside the scope and influence of OCORA.

Just when the first BB are realized or the OCORA architecture is significantly changed, the situation will occur that one BB must export some constraints or application rules (safety-related or non-safety-related), which hasn't 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 chapter of this whitepaper.

3.3 Recommendations for SRAC/AC application within OCORA

Based on the identified pain points of current SRAC/AC management, in this section, the OCORA collaboration provides general high-level recommendations for the application of SRACs/ACs within OCORA. The following list of recommendations is the result of a first brainstorming within the OCORA RAMS expert group. It has to be consolidated, reviewed and expanded. Additional recommendations have to be identified after finishing the OCORA architecture design.

- Deploy interaction between SRAC/AC emitters and receivers as much as possible. Try to involve the future receivers of SRAC/AC into the development loop to start "training" them on the required coverage from the beginning
- Provide typical coverage examples suitable for each SRAC/AC. The emitter should be able to provide examples of mechanisms to be deployed to cover the SRAC/AC (e.g. “verification” field on Figure 2). This should help the receiver at defining its own coverage.
- Clearly identify the system hazard for each SRAC. It is required in EN 50129 but not sufficiently challenged by ISA. A complete description shall be provided.
- OCORA has to define hazards that are 100% coverable at BB level (i.e. reuse data from Subset-091) to avoid SRAC emission because of non-fitted hazards to the system under consideration.
- OCORA has to define a standard list of SRACs/ACs to be deployed on the interaction of Building Blocks (BB) with outside onboard CCS scope. These SRACs/ACs can be standardized because they will rely on fully defined interfaces (OCORA, Subset, CONNECTA and other European initiatives).
- Avoid SRACs/ACs linked to "design" choice. These concern SRACs/ACs that are emitted because the technical mean to set-up at product level is so high that an SRAC/AC is emitted to give the receiver the activity to add it at this level. Among others, it concerns safety testing activities (e.g. periodic safety preventive maintenance) that shall be handle by the receiver's maintenance team. This kind of SRAC/AC are usually agreed between the emitter and the receiver.
- Define a generic definition of an AC so that everyone has the same understanding
- Well define SRACs/ACs (well described complete contextual information and addressed to an contextual recipient that does exist (SMART)) and relate each AC only to one topic
- Only forward SRACS/ACs that are worth forwarding (prevent from forwarding information, which is state of the art or ensured by resp. applied due to common measures or standards)
- Safety-related ACs shall have a clear safety-related context, that is, they shall be used to avoid, provide from or mitigate hazards that would arise, if the SRAC would not exist (SRACS shall not forward RAM-related or general information of system characteristics etc.)
- a SRAC, which is forwarded must be feasible to be realized for the receiver (no SRACs that are impossible or unreasonable to apply)
- as far as feasible to prevent resp. avoid a SRACs through design on level of the originating system, this shall be done (a SRAC shall only be created whenever a safety requirement cannot be implemented completely fulfilled by the system itself)
- SRAC have to be justified; SRAC receiver shall get all the necessary information to understand why it must be implemented, at which frequency the coverage mean shall be active etc. This information shall by provided by the SRAC emitter.

4 SRAC/AC Management in OCORA compliant projects

In this section an OCORA AC Template and a Management Guideline for the handling of non-standardized safety and non-safety related application conditions within OCORA compliant project is introduced. In general, OCORA Modular Safety Strategy aims to propose only standardized ACs between CCS-OB building blocks as well as between building blocks and integration levels, resulting from the OCORA safety requirements included in the OCORA CENELEC Documentation (see [11]).

Only in case all standardized ACs (if any) are already taken into account and the safety case cannot be closed the building block supplier (BBs) will have the possibility to formulate non-standardized SRACs to the integration level (SRACs/ACs between BB should be forbidden!). For these cases and because of the mentioned misunderstandings in today's SRAC process (see §2), the OCORA collaboration aims at improving the communication process between the Emitting Entities (EE) and Receiving Entities (RE) by proposing a standardized OCORA AC Template, a Management Guideline presented as a process flow chart between EE and RE and mandatory rules to be respected by all BB suppliers when defining non-standardized SRACs/ACs.

It must be noted, that non-standardized SRACs/ACs must be avoided as every non-standardized SRAC/AC decreases the interoperability and increases the efforts of recertification when it comes to evolution process (f.e. a BB has to be changed by another BB from another supplier, see [8])

The proposed OCORA AC Template as well as the OCORA AC Management Guidelines should be interpreted as a formal framework for SRAC/AC management within OCORA compliant projects. How these information and processes are implemented and concretized within the IT and/or organizational structure of the involved companies stays in the companies' responsibility.

4.1 OCORA AC Template

The OCORA AC Template, presented in Figure 4, shows some mandatory keywords (printed in bold) with an description which should be taken into account within the handling of ACs between the Emitting Entity (EE) and the Receiving Entity (RE). The process for filling out the template and for using it for an improved communication between EE and RE is proposed in 4.2.

OCORA AC Template
Filled out by the EMITTING ENTITY (EE):
Version - Version of AC (if suitable) **DateOfMod** - Date of last modification **Description** - Short description of the AC **Cat** - Category of AC: eg. Maintenance, Driver, Design.. **SRAC** - YES or NO Is this AC safety-related? Is the AC an SRAC? **Origin** - Where does the AC comes from? **Reason** - Why is this AC necessary? **Hazard** - For safety-related ACs; if not safety-related: impact on RAM **EE_Contact** - Contact person of the Emitting Entity **RE_Contact**- Contact person within the Receiving Entity **ExOfCoverage** - How can this AC be covered (just informative)
Filled out by the RECEIVING ENTITY (RE):
RespManager - Responsible manager for coverage (defined by the receiver) **WayOfCoverage** - Describe the Way of Coverage **Monitoring** - Decribe the way the effectiveness of the AC ca be monitored if its effectiveness is not fully clear (optional) **Covered** - YES or NO - ACs fully implemented/covered? **Mitigation** - What if the SRAC is not covered? Solution for mitigation?

Figure 4 Template for handling with non-standardized application Conditions (ACs) within OCORA

4.2 OCORA AC Management Guideline

The process how to handle with non-standardized application conditions (ACs) within OCORA by using the OCORA AC template shown in the following Figure 5.

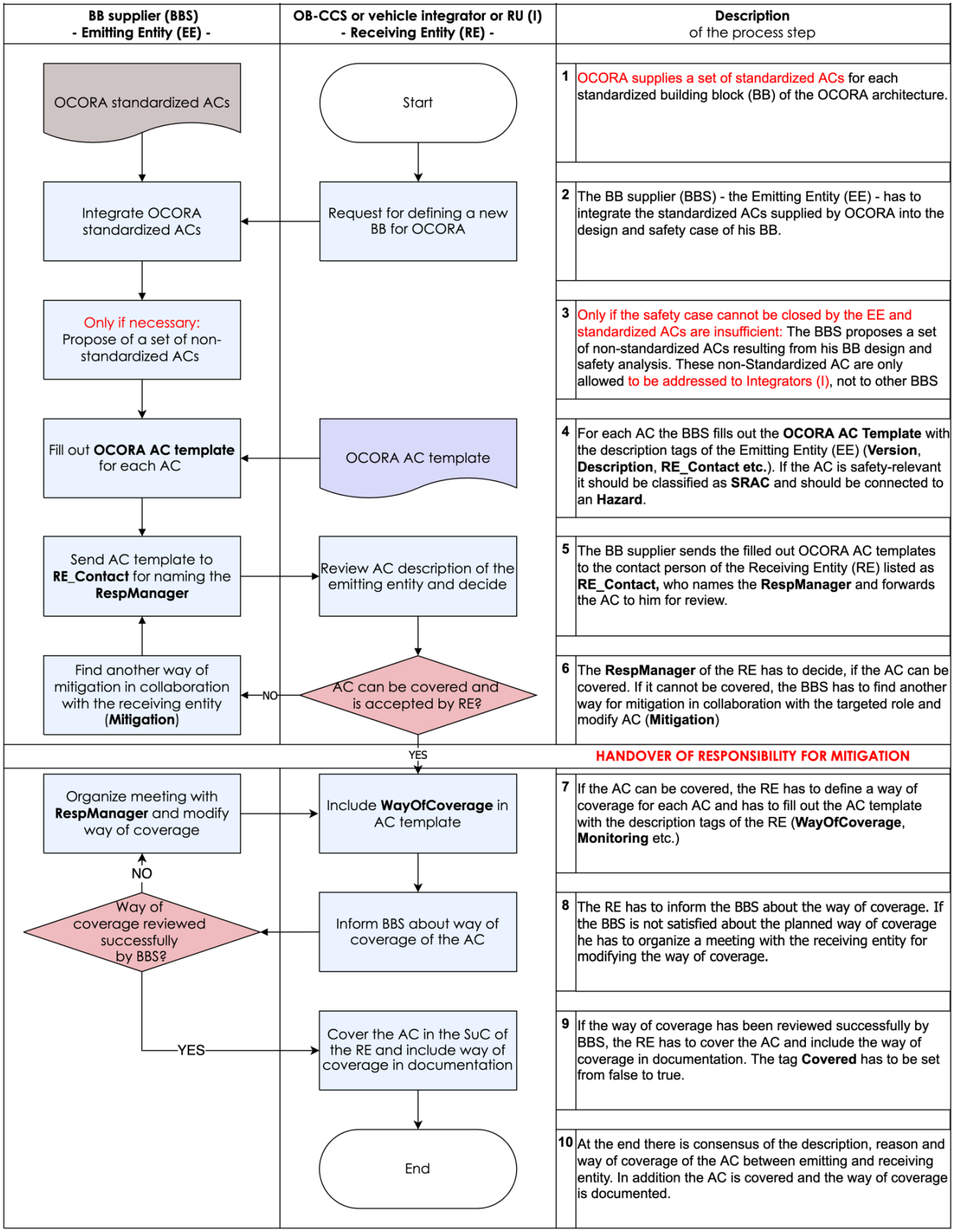

Figure 5 Handling of non-standardized application conditions (ACs) within OCORA

It must be noted that this consultation presented in **step 6** of the process in Figure 5 between BBS and the RE has only be performed by the first use of the BB. When the BB is already certified the set of ACs cannot be challenged anymore.
Secondly, a distinction must be made between the responsibilities of each side (EE resp. RE). The BBS is responsible for the AC definition (**steps 1-6** in Figure 5) and the RE for its coverage (**steps 7-10** in Figure 5, as it is today the case). The OCORA collaboration provides means to avoid grey areas between EE and RE.

4.3 Outlook on further deliverables

Resulting from the OCORA CENELEC documentation, the following deliverables will be developed by the OCORA RAMS team and presented within the next OCORA Releases:

- For following the goal of the OCORA Modular Safety strategy, a OCORA Standardized AC list to be deployed on the interaction of different Building Blocks (BB) together and with the external world will be proposed. These SRACs/ACs can be standardized because they will rely on fully defined interfaces (OCORA, ERTMS Subsets, CONNECTA and other European initiatives),
- Furthermore, OCORA Non-standardized ACs definition rules will be proposed for defining a framework in which non-standardized SRACs/ACs are allowed to be defined within OCORA (SRACs must not go against modularity) in addition to the defaults given by the OCORA AC template and OCORA AC management guideline.