OCORA

Open CCS On-board Reference Architecture

RAMS – Evolution Management

Document ID: OCORA-TWS07-020

Version: 2.20

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	JB	01.08.2021
1.01	Definition of the document structure based on the R1 template	JB	03.11.2021
1.02	Update according to member review. Complete all section	JB	11.11.2021
1.03	Update following Modular Safety reviews	JB	17.11.2021
2.00	Official version for OCORA Release R1	JB	18.11.2021
2.10	First draft for OCORA R2	JB	10.05.2022
2.20	Update following comments Official release	JB	09.06.2022

Table of contents

1 Introduction 5

1.1 Purpose of the document 5

1.2 Applicability of the document 5

1.3 Context of the document 6

2 Context of Evolution management 7

2.1 Current situation regarding CCS-OB evolutions 7

2.2 Methodology deployed to develop evolution management 9

2.3 Existing regulations related to evolution management 11

2.4 Scope of “evolution management” in OCORA 14

2.4.1 Definition of “evolution” within OCORA compliant systems 14

2.4.2 Scope of the current evolution management process 14

2.5 Benefits of evolutions in a modular architecture 17

2.6 Concept of “safe integration” 17

2.7 ISA activities for OCORA evolved systems 21

3 Significance process and matrix 23

4 Test impact process and matrix 28

4.1 First delivery of the CCS on board system 30

4.2 Update of building blocks 30

4.3 Addition of a new building block in the CCS-OB 31

4.4 Removal of a building block in the CCS-OB 31

Table of figures

Figure 1 OCORA RAMS Strategy and RAMS Documentation 6

Figure 2 Current example of CCS-OB evolution through its life cycle 8

Figure 3 SUBSET-026 overall vision for ERTMS systems 9

Figure 4 Evolution process methodology 10

Figure 5 OCORA CCS-OB architecture [8] 15

Figure 6 Evolutions management top level process 16

Figure 7 Current ERTMS approval process 18

Figure 8 ERTMS approval process including OCORA 19

Figure 9 Significance process for the building blocks evolution 23

Figure 10 Failure consequence sub-process 24

Figure 11 Significance matrix 25

Figure 12 Diagram of Safety Significance Analysis from EN 17023 [19] 27

Figure 13 Overall evolution process representation 29

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.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

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

[6] OCORA-BWS03-020 - Guiding-Principles

[7] OCORA-BWS04-010 – Problem Statements

[8] OCORA-TWS01-030 – System Architecture

[9] OCORA-TWS05-021 – Program Requirements

[10] OCORA-TWS07-010 –Safety Strategy

[11] OCORA-TWS09-010_Testing-Strategy

[12] OCORA-TWS07-040 - Optimized Approval Process

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

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

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

[16] EN 50657: 2017 - Railways Applications - Rolling stock applications - Software on Board Rolling Stock

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

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

[19] EN 170.23: 2018 - Railway applications - Railway vehicle maintenance - Creation and modification of maintenance plan

[20] EN 50506-2: 2009 - Railway applications — Communication, signalling and processing systems — Application guide for EN 50129 - Part 2: Safety assurance

[21] 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

[22] CSM-RA - common safety method for risk evaluation and assessment and repealing Regulation (EC) 402/2013

[23] Directive 2018/545 - COMMISSION IMPLEMENTING REGULATION (EU) 2018/545 of 4 April 2018 establishing practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process pursuant to Directive (EU) 2016/797 of the European Parliament and of the Council

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

[25] D RTE 49100 - Nachweisführung bei Änderungen an Eisenbahnfahrzeugen (de)/ Démonstration lors de modifications sur des véhicules ferroviaires (fr)

1 Introduction

1.1 Purpose of the document

This document, started in the OCORA Delta and to be continued in further OCORA releases, covers the following aspects:

- Analysis of the current standards and directives regarding evolutions management of CCS OB systems (refer to section 2),
- Proposition of a new generic approach to determine the significance of evolutions in OCORA compliant CCS OB systems (refer to section 3),
- Proposition of a new generic approach to determine the minimum required testing activities to be performed when dealing with evolutions in OCORA compliant CCS OB systems (refer to section 4). This topic is initiated in OCORA R2 but will be developed in future OCORA releases.

The purpose of this document is to address a systematic approach when realising evolution on building blocks and spreading them through the whole railway assessment Lifecyle up to the final vehicle authorisation as defined in Directive 2018/545 [23]. This document provide means against one main issue defined in Problem Statements [7]:

Current ETCS On-board solutions:

[…]

*4. are **difficult and time consuming to adapt/change/update/upgrade**:*

- *In the case of patching in non SIL area (e.g. cyber- security patching)*
- *In the case of error correction in SIL area*
- *In the case of baseline upgrade (e.g. ETCS baseline 2 to 3)*
- *In the case of functional enrichment (ex. base for game changer introduction is not a given)*

[…]

Based on the previous problem statement, it aims at covering the following expected result defined in Introduction to OCORA [5]:

*3. Robust interface specifications allowing for **smooth evolution** and migration.*

“Evolution” in the scope of OCORA RAMS refer to a change of an OCORA compliant system once it has been certified. A more complete definition is provided in section 2.4.1.

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, introduced in OCORA Modular Safety Strategy [10], 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 [7]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

The Whitepaper on Evolution 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.

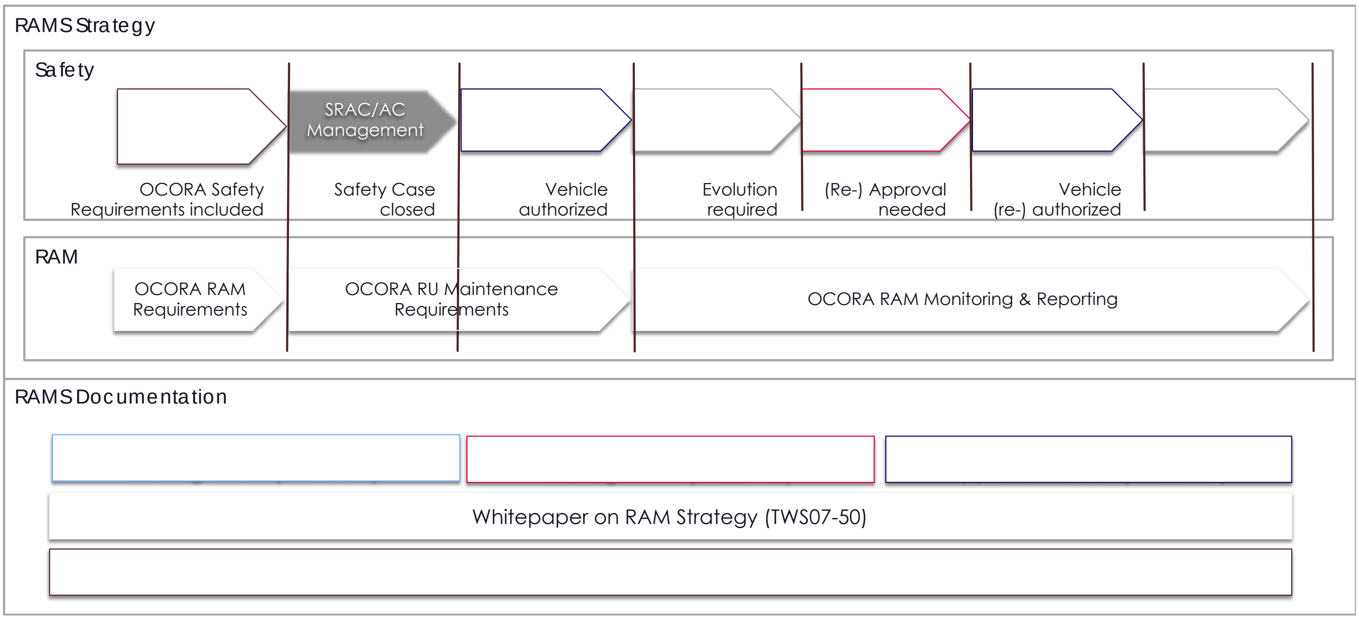


Figure 1 OCORA RAMS Strategy and RAMS Documentation

2 Context of Evolution management

2.1 Current situation regarding CCS-OB evolutions

Railway products or systems use to have a life cycle up to 30 years. Therefore, between the first version of an equipment installed in its operational environment (i.e. refer to Phase 11 of the CENELEC V cycle of EN 50126-1 [13]) and the decommissioning/disposal phase (i.e. refer to Phase 12), it will likely evolve by adding new functionalities, correcting defects, providing improvements etc.

Safety critical systems in the ERTMS environment (e.g. CCS-OB) have to be defined according to the TSI CCS [21]. This considers the technical requirements defined by the different SUBSETS and the CENELEC standards (i.e. EN 50126 [13], EN 50128 [15] [for the CCS-OB], EN 50657 [16] [for the Train Adapter] and EN 50129 [17]) plus all the additional standards referred in these three main ones (e.g. EN 50159 [18]).

The conformity of the CCS-OB according to these standards is based on the technical documents provided by the manufacturer whose overall summary is presented in the safety case.

Its structure and content are presented in section 7 of EN 50129 [17] where the first section requires that:

> *Part 1 — Definition of system*
>
> *This shall precisely define or reference the system, subsystem or equipment to which the Safety Case refers, including version numbers and modification status of all requirements, design and application documentation.*

This states that the CCS-OB covered by an ISA certificate corresponds to a frozen picture of it. Fundamentally, no further modification is possible without the realization of a new release of the safety case, which will lead to finally get a new certificate for the CCS-OB.

Over the whole life cycle of a CCS-OB system, this will likely happen several times and the costs related to the recertification activities are typically very high and prevent a lot of evolutions which could improve the overall performances of the CCS-OB. Indeed, most of the time, the ratio costs vs benefits of the evolutions are not worth realizing it from a business point of view. This statement is just a quick summary of the complete CCS risk profile analysis realized in Introduction to OCORA [5]. These documents states that:

> *The volatility of the CCS system for the railway community at large because of e.g. frequent updates of the specification and technological developments, but also the variability of user specifications, resulting in an average life cycle expectancy for CCS systems of 5 to 10 years with an average of, currently, about 6 years. The net result of this development is, that rolling stock has to be retrofitted several times during its (residual) lifecycle. For new rolling stock fitted with ERTMS and with a life expectancy of +30 years, this would mean at least 4 consecutive retrofits. The CCS market will, therefore, be dominated by the need for retrofits and not by newly built requirements.*

This happens today because of a monolithic approach of the CCS-OB, presented on Figure 3, prevent smooth changes, especially when dealing with proprietary hardware. Thus, from a manufacturer's business strategy, it worth accumulating a maximum of evolutions into sustaining baselines (including new hardware). In that case, the CCS-OB (and thus its safety case and certificate) evolve only by big steps. This is represented in the example on Figure 2.

Manufacturers use to collect a large number of change requests from their customers linked to (not exhaustive):

- minor non-critical defects (e.g. RAM target not reached),
- improvements (e.g. more accurate events to be logged in memory for preventive and corrective maintenance),
- obsolescence management (e.g. exchange of hardware components where end of life is programmed by their manufacturers),

before considering that an update of the CCS OB system update worth it from business point of view and especially from certification point of view (as explained above). Whatever the scope of the assessment is, the "entry ticket" uses to be high because of preparation of documents, involvement of the assessor in preliminary meetings, documentation to be shared… This directly increases the cost of the "small" evolutions presented above for the customers and most of the time, they will decline that and wait for a future merged baseline with other customers to have a better repartition of the cost among them.

Usually, the case where the current CCS OB system are updated without delays are when:

- new functionalities are requested (e.g. implementation of SUBSET-119 for TSI 2022) and obviously will be present into the next call for tenders,
- critical change requests (e.g. safety issue raised by one or several customer) where a retrofit must be done in the shortest time possible on all deployed equipments).

Beside these two cases, the customers use to wait months or even years before having their other change requests integrated into a new version of the CCS OB system.

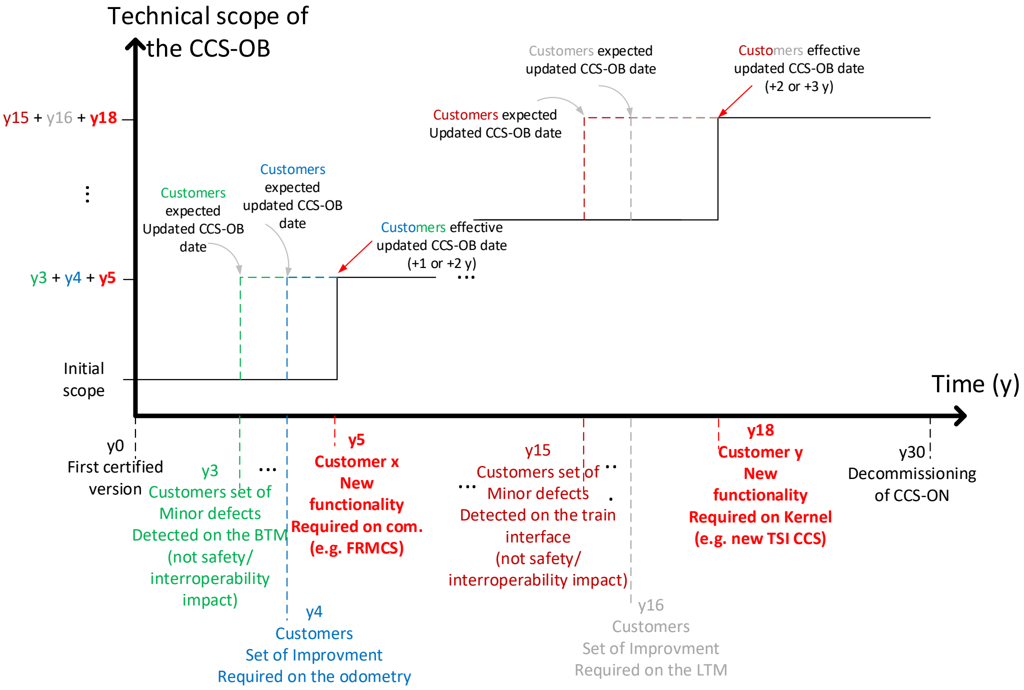
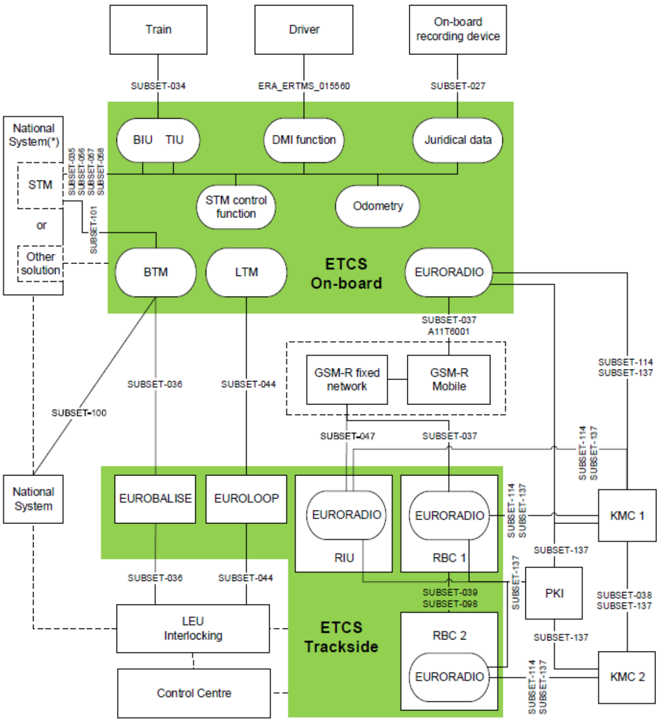

Technical scope of the CCS-OB
y15 + y16 + y18
⋮
y3 + y4 + y5
Initial scope
Time (y)
Customers expected Updated CCS-OB date
Customers expected updated CCS-OB date
Customers effective updated CCS-OB date (+1 or +2 y)
…
Customers expected Updated CCS-OB date
Customers expected updated CCS-OB date
Customers effective updated CCS-OB date (+2 or +3 y)
y0
First certified version
y3
Customers set of Minor defects Detected on the BTM (not safety/ interroperability impact)
…
y4
Customers Set of Improvment Required on the odometry
y5
Customer x
New functionality
Required on com.
(e.g. FRMCS)
…
y15
Customers set of Minor defects Detected on the train interface (not safety/ interroperability impact)
…
y16
Customers Set of Improvment Required on the LTM
y18
Customer y
New functionality
Required on Kernel
(e.g. new TSI CCS)
y30
Decommissioning of CCS-ON

Figure 2 Current example of CCS-OB evolution through its life cycle

An additional reason of this “big steps” approach when managing evolutions is that current CCS-OBis mostly composed by the ETCS On-board (refer to Figure 3). The ETCS-OB system covers different critical functions in a single overall safety case. Because of that, any update that is claimed in a function will impact the whole safety case and certificate.



(*) Depending on its functionality and the desired configuration, the national system can be addressed either via an STM using the standard interface or via another national solution

Figure 3 SUBSET-026 overall vision for ERTMS systems

Safety activities in railway sectors represent a large part of the overall system costs during the whole lifetime. The previous statement about the slow evolutions of the CCS-OB system is also applicable:

- when safely integrating the technical equipment into one or several train types,
- when safely integrating a fleet to a dedicated network.

All these activities aim at getting a “vehicle authorization for placing on the market” as required by the European directive 2018/545 [23]. This is the mandatory condition for a railway undertaking (or another entity) to use a train on a railway network.

The process described in this document, which includes the modular approach and architecture from OCORA, will allow to do “smaller steps” (update, change, evolution etc. identified in dashed lines on Figure 2) of the CCS-OB in terms of vehicle authorization when the RU/operator requires it. These “smaller steps” will not systematically require to be applied for new vehicle authorization (e.g. none-safety critical modifications). **The objective of this process is to limit at maximum the need of complete retrofit once a train is equipped with an OCORA compliant CCS-OB by only performing evolutions on the latter in its constituting independent building blocks.**

2.2 Methodology deployed to develop evolution management

Prior developing this evolution process, it is important to describe the methodology used as a roadmap. The latter is presented on Figure 4.

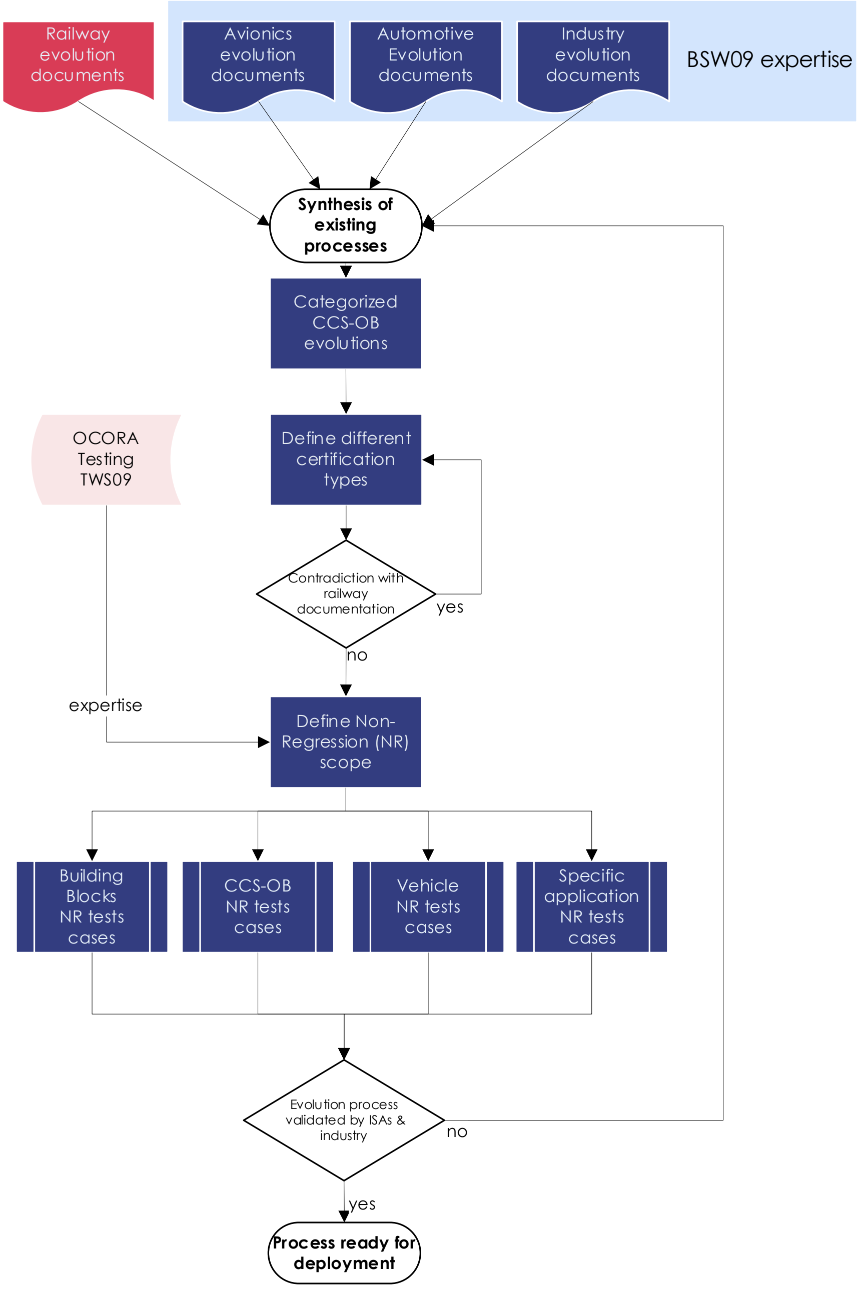

Railway evolution documents
Avionics evolution documents
Automotive Evolution documents
Industry evolution documents
BSW09 expertise
Synthesis of existing processes
Categorized CCS-OB evolutions
OCORA Testing TWS09
Define different certification types
Contradiction with railway documentation
yes
no
expertise
Define Non-Regression (NR) scope
Building Blocks NR tests cases
CCS-OB NR tests cases
Vehicle NR tests cases
Specific application NR tests cases
Evolution process validated by ISAs & industry
no
yes
Process ready for deployment

Figure 4 Evolution process methodology

This methodology is based around 4 main steps:

1. Research of existing railway documentation applicable when dealing with evolutions:
    a. Railway documentation under consideration is identified in §2.3,
    b. Avionics sector based on the IMA (Integrated Modular Avionics) deployed for decades now with, for instance, the deployment of the AHP (Analytic Hierarchy Process) methodology. This should be further developed in future OCORA releases. So far, up to R2, no useful documentation regarding evolution was found,
    c. Automotive sector where modularity, upgradability and evolvability are key aspects of this very competitive market. This should be further developed in future OCORA releases. So far, up to R2, no useful documentation regarding evolution was found.,
    d. Industry sector (e.g. https://www.fairphone.com/en/). This should be analyzed in future OCORA releases; it is not considered up to OCORA R2.

    The activity of analyzing other sectors standards is the task of the BWS09 – Acceptance of Global Standards group. Up to R2, this group focuses on the railway sector. In the future they should analyze additional sectors standards that could benefit, in a second step, to the evolution management.

When the research is over, a summary of the analyzed documents is provided and presents:

e. The redundancy between the different processes (if any),

f. The strengths of each process,

g. The weaknesses of each process,

h. Its adaptability to the railway world.

2. The second step consists in defining which type of evolutions in the CCS-OB system are covered by the process. This is presented in §2.4 and illustrated on Figure 13.
3. One key activity of this process is to propose different shades of assessments based on the evolution impact. This is presented in §2.7.
4. For the last step, the Testing group of OCORA (i.e. TWS09) will join the RAMS team (i.e. TWS08) to define a typical scope of non-regression tests for each type of classified evolutions:

   a. For each building block or type of building blocks (L2)(this will be clarified in a future release of OCORA),

   b. For the CCS-OB (L3) integrating the evolved building block(s),

   c. For the vehicle hosting the CCS-OB (L4) through the Train Adapter defined by OCORA,

   d. For the specific application represented (L5) by the vehicle in its dedicated network. The vehicle authorization, as required by Directive 2018/545 [23] is done at this final step.

   The different integration levels (i.e. L1 to L5) are defined in the OCORA Testing Strategy [11].

   Obviously, the mandatory non-regression test scope becomes more and more simplified when moving from building block validation to the vehicle/network integration phase. This is presented in details in section 4. One main goal of OCORA integration activities, defined in the Program Requirements document [9] is to avoid, at maximum, without degrading safety, redundant and not relevant non-regression activities when dealing with evolutions.

After each step, a check will be done to ensure that what has been achieved so far presents no contradiction or incompatibilities with existing railway standard or directive.

When the process will be judged as mature, it will be share to a selected panel of accredited assessors (i.e. ISA, NoBo, DeBo, AsBo) for review. Once comments have been taken in account, it will be delivered in another document as the reference set of documents for OCORA compliant program certification.

2.3 Existing regulations related to evolution management

The case of retrofitting current trains equipped with monolithic CCS-OB with new OCORA ones is not the purpose of this process. This will be addressed in the Optimized Approval Process [12] which is a complementary document to be applied after the evolution management process (refer to [12]).

In today’s standard related to the interoperability world, directive CSM-RA [22] provides a unified methodology in Europe for managing safety activities in case of evolution of a system covered by a Vehicle Authorization as defined in Directive 2018/545 [23].

CCS-OB is basically covered by its scope in CSM-RA [22]:

> *Article 2*
> *Scope*
>
> *3. This Regulation shall apply also to structural sub-systems to which Directive 2008/57/EC applies:*

(a) if a risk assessment is required by the relevant technical specification for interoperability (TSI); in this case the TSI shall, where appropriate, specify which parts of this Regulation apply; (see 3.2 below)

Extract from TSI CCS [21]:
3.2. Specific Aspects of the Control-Command and Signalling Subsystems
3.2.1. Safety
Every project to which this specification is applied shall take the measures necessary to ensure that the level of risk of an incident occurring within the scope of the Control-Command and Signalling Subsystems, is not higher than the objective for the service. For this purpose the Commission Implementing Regulation (EU) No 402/2013 (1), as referred to in Article 6(3)(a) of Directive 2004/49/EC (Common Safety Method), applies.

Extract from CSM-RA [22]: *(b) if the change is significant as set out in Article 4(2), the risk management process set out in Article 5 shall be applied within the placing in service of structural sub-systems to ensure their*
safe integration into an existing system, by virtue of Article 15(1) of Directive 2008/57/EC.

Extract from CSM-RA [22]:*ANNEX I*
1. GENERAL PRINCIPLES APPLICABLE TO THE RISK MANAGEMENT PROCESS
1.1. General principles and obligations

*1.1.4. The **actors who already have in place methods or tools for risk assessment may continue to apply** them if such methods or tools are compatible with the provisions of this Regulation and subject to the following conditions:*

(a) the risk assessment methods or tools are described in a safety management system accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC; or

*(b) **the risk assessment methods or tools are required by a TSI** or comply with publicly available recognised standards specified in notified national rules.*

In addition to CSM-RA [22], CENELEC standard EN 17023 [19] has also been analysed during this whitepaper realisation. Indeed, the latter uses the same criteria, with the same definition, as defined in CSM-RA [22] but with more contextual data, processes and detailed examples of combination between the criteria:

> *A.1 General*
>
> *[…]*
>
> *The Article 4 of the Regulation (EU) 402/2013 indicates that, when the proposed change has an impact on safety, the proposer shall decide, by expert judgement, the significance of the change based on the following criteria:*
>
> > *a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;*
> >
> > *b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organization implementing the change;*
> >
> > *c) complexity of the change;*
> >
> > *d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and*
> >
> > *take appropriate interventions;*
> >
> > *e) reversibility: the inability to revert to the system before the change;*
> >
> > *f) additionality: assessment of the significance of the change taking into account all recent safety-*
> >
> > *related modifications to the system under assessment and which were not judged as significant.*
>
> *NOTE The Regulation (EU) 402/2013 uses the term change and this standard uses the specific term modification.*

Based on the previous statement, usually two different strategies are developed by the manufacturers:

- Apply the CSM-RA directive [22] and EN 17023 [19] with the use of "significant" and "non-significant" modifications which drive at the end to the edition (i.e. for significant changes) or not (i.e. for non-significant changes) of a new certificate for the CCS-OB or,
- Apply the CENELEC development process as allowed by ANNEX I 1.1.4 (b) of CSM-RA [22] where the modifications management are presented in EN 50129 [17]:

1 Scope

[...]

This document is not applicable to existing systems, subsystems or equipment which had already been accepted prior to the creation of this document. However, so far as reasonably practicable, it should be applied to modifications and extensions to existing systems, subsystems and equipment.

[...]

8.3 Modification and retrofit

During the operational life of a system, change requests can be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation.

Where a change request results in a modification which could affect the safety of the system, or associated systems, or the environment, the appropriate portion of the safety life cycle shall be repeated to ensure that the implemented modification does not unacceptably reduce the level of safety.

Modifications shall be controlled using the same quality management, safety management and functional/technical safety criteria as would be used for a new design. All relevant documentation, including the Safety Case, shall be updated ***or supplemented by additional documentation****.*

Based on the last segment “or supplemented by additional documentation”, the present document aims at proposing additional systematic means for managing evolutions without necessarily update the CCS-OB or its constituent safety cases, depending on their criticality. This is the entry point for this evolution process.

2.4 Scope of “evolution management” in OCORA

2.4.1 Definition of “evolution” within OCORA compliant systems

The term “evolution” in defined in the Glossary [2]. This whitepaper refers to the evolutions of a CCS-OB system or its constituting building blocks that have already been certified according to:

- NoBo independent conformity assessment defined in TSI CCS [21]
  - Interoperability certificate (i.e. design examination certificate),
  - ISA certificate (i.e. compliance to CENELEC standards),
- DeBo examination report (only when dealing with NNTR),
- OCORA requirements (this will be defined in the Optimized Approval Process [12]).

These “evolutions” refers to a delta of one or several elements contained into the technical file of the SuC which is presented into the safety case between the last certified version and the current one. Evolutions can be safe and non-safe as presented in section 3 .

Evolutions are a central key element of OCORA to reach the seven design goals defined in Guiding Principles [6]:

- ***Openness***
- ***Modularity***
- ***Exchangeability***
- ***Migrateability***
- ***Evolvability***
- ***Portability***
- ***Security***

2.4.2 Scope of the current evolution management process

Evolutions managed in this whitepaper are mostly related to the CCS-OB and the Train Adapter as described in the System Architecture document [8]. They are represented by the green and blue frame on Figure 5.

It must be noticed that the train adapter will, on a longer run, not be useful anymore and therefore removed. The convergence of vehicle networks, consisting of one or multiple bus systems that integrate the CCS and vehicle bus systems is already under scrutiny of OCORA and Shift2Rail Connecta. This is presented into the Introduction to OCORA [5]. The upper levels of the overall system (i.e. Vehicle level and system level) are also considered in the present process with a more limited impact than at building block and CCS-OB levels. These levels will be more developed into the Optimized Approval Process [12].

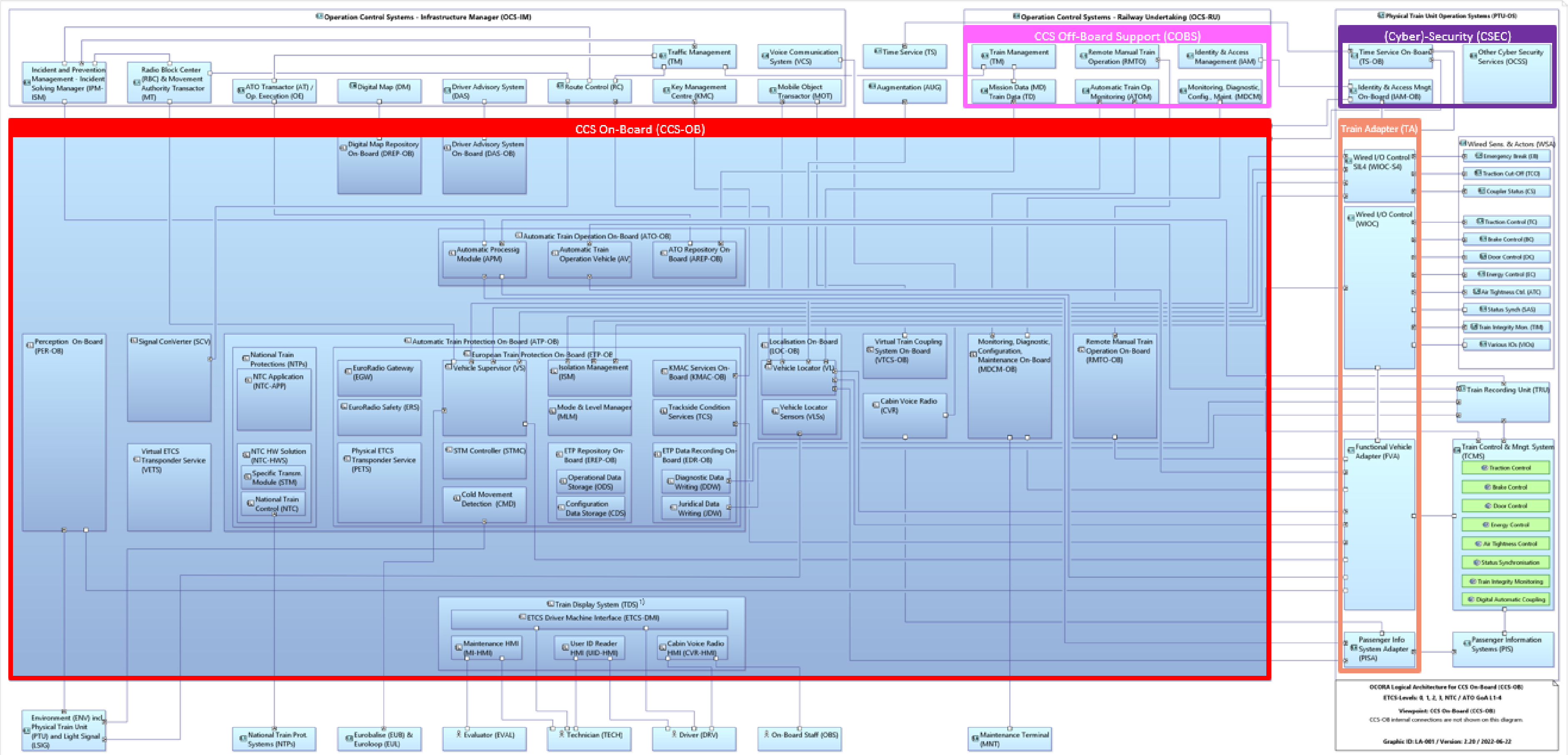
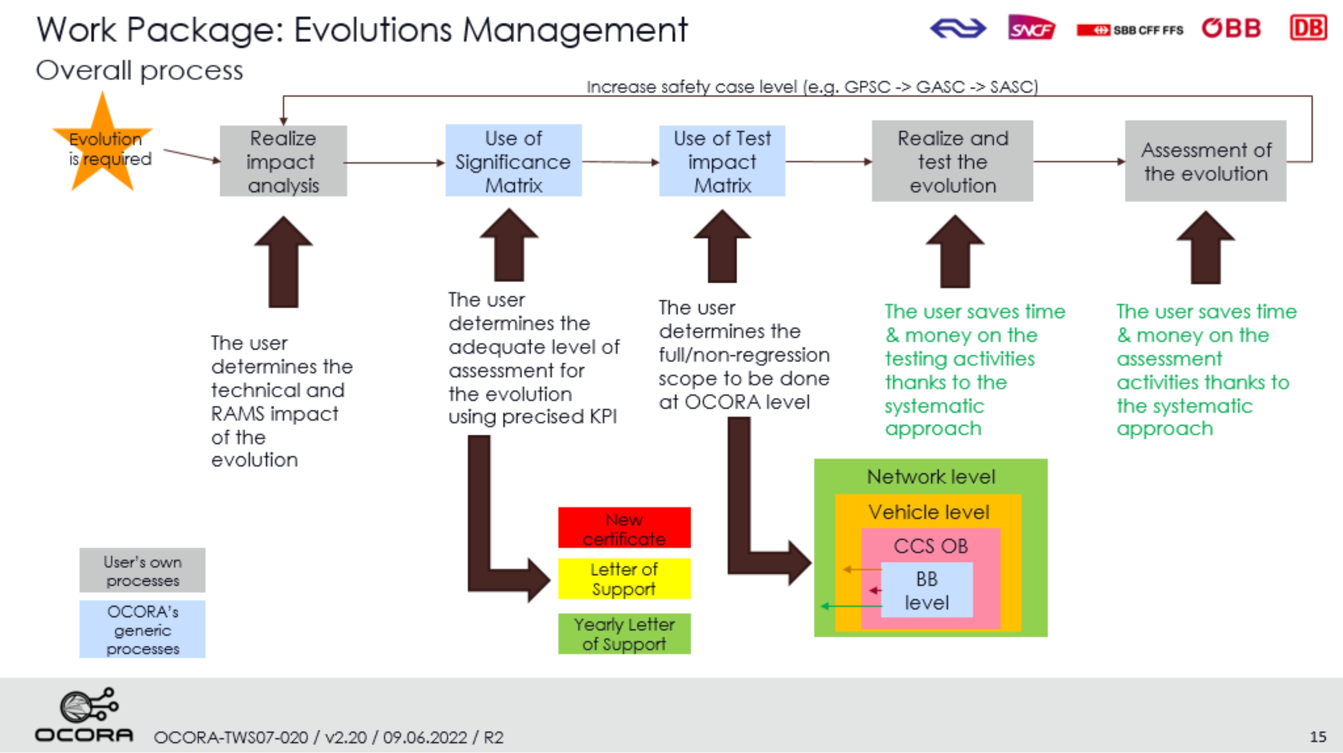

Operation Control Systems - Infrastructure Manager (OCS-IM)
Incident and Prevention Management - Incident Solving Manager (IPM-ISM)
Radio Block Center (RBC) & Movement Authority Transactor (MT)
ATO Transactor (AT) / Op. Execution (OE)
Digital Map (DM)
Driver Advisory System (DAS)
Route Control (RC)
Traffic Management (TM)
Key Management Centre (KMC)
Voice Communication System (VCS)
Mobile Object Transactor (MOT)
Time Service (TS)
Augmentation (AUG)
Operation Control Systems - Railway Undertaking (OCS-RU)
CCS Off-Board Support (COBS)
Train Management (TM)
Remote Manual Train Operation (RMTO)
Identity & Access Management (IAM)
Mission Data (MD) Train Data (TD)
Automatic Train Op. Monitoring (ATOM)
Monitoring, Diagnostic, Config., Maint. (MDCM)
Physical Train Unit Operation Systems (PTU-OS)
(Cyber)-Security (CSEC)
Time Service On-Board (TS-OB)
Other Cyber Security Services (OCSS)
Identity & Access Mngt On-Board (IAM-OB)
CCS On-Board (CCS-OB)
Digital Map Repository On-Board (DREP-OB)
Driver Advisory System On-Board (DAS-OB)
Automatic Train Operation On-Board (ATO-OB)
Automatic Processig Module (APM)
Automatic Train Operation Vehicle (AV)
ATO Repository On-Board (AREP-OB)
Perception On-Board (PER-OB)
Signal ConVerter (SCV)
Virtual ETCS Transponder Service (VETS)
Automatic Train Protection On Board (ATP-OB)
National Train Protections (NTPs)
NTC Application (NTC-APP)
NTC HW Solution (NTC-HWS)
Specific Transm. Module (STM)
National Train Control (NTC)
European Train Protection On-Board (ETP-OB
EuroRadio Gateway (EGW)
EuroRadio Safety (ERS)
Physical ETCS Transponder Service (PETS)
Vehicle Supervisor (VS)
STM Controller (STMC)
Cold Movement Detection (CMD)
Isolation Management (ISM)
Mode & Level Manager (MLM)
ETP Repository On-Board (EREP-OB)
Operational Data Storage (ODS)
Configuration Data Storage (CDS)
KMAC Services On-Board (KMAC-OB)
Trackside Condition Services (TCS)
ETP Data Recording On-Board (EDR-OB)
Diagnostic Data Writing (DDW)
Juridical Data Writing (JDW)
Localisation On-Board (LOC-OB)
Vehicle Locator (VL)
Vehicle Locator Sensors (VLSs)
Virtual Train Coupling System On-Board (VTCS-OB)
Cabin Voice Radio (CVR)
Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB)
Remote Manual Train Operation On-Board (RMTO-OB)
Train Display System (TDS) 1)
ETCS Driver Machine Interface (ETCS-DMI)
Maintenance HMI (MI-HMI)
User ID Reader HMI (UID-HMI)
Cabin Voice Radio HMI (CVR-HMI)
Train Adapter (TA)
Wired I/O Control SIL4 (WIOC-S4)
Wired I/O Control (WIOC)
Functional Vehicle Adapter (FVA)
Passenger Info System Adapter (PISA)
Wired Sens. & Actors (WSA)
Emergency Break (EB)
Traction Cut-Off (TCO)
Coupler Status (CS)
Traction Control (TC)
Brake Control (BC)
Door Control (DC)
Energy Control (EC)
Air Tightness Ctrl. (ATC)
Status Synch (SAS)
Train Integrity Mon. (TIM)
Various IOs (VIOs)
Train Recording Unit (TRU)
Train Control & Mngt. System (TCMS)
Traction Control
Brake Control
Door Control
Energy Control
Air Tightness Control
Status Synchronisation
Train Integrity Monitoring
Digital Automatic Coupling
Passenger Information Systems (PIS)
Environment (ENV) incl. Physical Train Unit (PTU) and Light Signal (LSIG)
National Train Prot. Systems (NTPs)
Eurobalise (EUB) & Euroloop (EUL)
Evaluator (EVAL)
Technician (TECH)
Driver (DRV)
On-Board Staff (OBS)
Maintenance Terminal (MNT)
OCORA Logical Architecture for CCS On-Board (CCS-OB)
ETCS-Levels: 0, 1, 2, 3, NTC / ATO GoA L1-4
Viewpoint: CCS On-Board (CCS-OB)
CCS-OB internal connections are not shown on this diagram.
Graphic ID: LA-001 / Version: 2.20 / 2022-06-22

Figure 5 OCORA CCS-OB architecture [8]

From a process point of view the evolution management process focuses on the two mains steps presented in blue on the figure below:



Work Package: Evolutions Management

Overall process

Increase safety case level (e.g. GPSC -> GASC -> SASC)

Evolution is required

Realize impact analysis

Use of Significance Matrix

Use of Test impact Matrix

Realize and test the evolution

Assessment of the evolution

The user determines the technical and RAMS impact of the evolution

The user determines the adequate level of assessment for the evolution using precised KPI

The user determines the full/non-regression scope to be done at OCORA level

The user saves time & money on the testing activities thanks to the systematic approach

The user saves time & money on the assessment activities thanks to the systematic approach

New certificate

Letter of Support

Yearly Letter of Support

Network level

Vehicle level

CCS OB

BB level

User's own processes

OCORA's generic processes

OCORA-TWS07-020 / v2.20 / 09.06.2022 / R2 15

Figure 6 Evolutions management top level process

This process is composed of the following steps:

- An evolution is required: either the BB supplier has identified a need to update its system (e.g. new OCORA requirements, bug fixing) or the vehicle owner requires a change in the CCS-OB constitution (e.g. new BB, change of supplier for a BB).
- Realize impact analysis: this activity, performed by the user with his own process, aims at defining the impact of the modification from a technical point of view (e.g. system, SW/HW engineering). Evolutions must be handled in the user's change management database as well as any other evolution (i.e. not in OCORA scope).
- Use of significance matrix: this tool, defined by the RAMS group aims at determining the relevant level of assessment required based on the technical impact analysis. This is presented in section 3.
- Use of test impact matrix: this tool, defined jointly with the RAMS and Testing groups aims at defining the different scopes of non-regression testing to be performed depending on the evolutions' impacts (i.e. which OCORA interfaces are impacted and non-impacted). This will help each user to easier define the testing strategy at his level but also for all above levels. This will be fully explained in a future version of the Testing Strategy [11] and introduced in section 4.
- Realize and test the evolution: this activity, performed by the user with its own process, represents the implementation of the evolution and then its testing.
- Assessment of the evolution: this activity, performed by the user with its own process, represents the assessment of the evolution with an assessor.

When the BB has been successfully re-assessed, the process is looped and starts again with increasing one level: CCS-OB, then vehicle level and finally system level. When dealing with these levels, the Optimized Approval process [12] must be used in a second step as a complementary document to ensure that the whole chain of safety activities benefits from the modular approach.

2.5 Benefits of evolutions in a modular architecture

The general benefits of deploying a modular architecture in the CCS-OB systems are presented in Introduction to OCORA [5]. In accordance with OCORA expected benefits, this document tends to provide benefits for all the stakeholders involved into OCORA compliant programs thanks to smooth evolutions:

Manufacturers: The standardization of different certification levels requiring different shades of documentation to be updated aims at avoiding a systematic new certificate request to the assessor (see §2.6. This will greatly ease the management of ”small” evolutions (e.g. non safe functions in non-segregated building blocks [between safe and non-safe parts], change of non-critical item inside a safe part). The way to quantify “small” evolutions is described in the “Significance Matrix” in Figure 11.

- Integrators (i.e. at CCS-OB, vehicle and system levels as defined in the Testing Strategy [11]): The evolution management process defines standardized non-regression tests based on the evolutions under consideration. These scopes, in addition to the specific tests procedures check the modification itself, aim at accelerating the evolved building blocks or CCS-OB at their integrated level. This is possible because individual analyses for non-regression activities will be avoided.
- Assessors: The current evolution process will be submitted to several ISA for their approval. This will be done when the present document will be finalized. The benefit for them is that this process provides clear frames for the different certification levels (i.e. not to be re-defined for each evolution) which means more frequent updates of the certified systems but with a clear defined assessment scope.
- Railway Undertakings: The process allows to accelerate the update of the deployed vehicles equipped with OCORA compliant systems and reduce drastically costs. The “big steps” as presented on Figure 2 will be replaced by more frequent “small steps” composed of minor evolutions with strong benefits in time and costs development for the projects, close to evolutions of other rolling stock systems.

It must be noticed that all the benefits presented above must not degrade the overall RAMS level of the different projects. It may at the opposite reinforce it. The objective behind it is that it is considered safer to handle smaller but more frequent updates following a systematic approach rather than important ones, less frequent but with a wider and more complex scope.

2.6 Concept of “safe integration”

The decomposition of the current CCS-OB system as defined by TSI CCS [21] and represented on Figure 3 introduces two new actors whose tasks are today mostly intrinsically covered by the train manufacturers. The most common current ERTMS approval process is synthetized on Figure 7. Other possible organizations are possible depending of the repartition of the roles by the contracting entity.

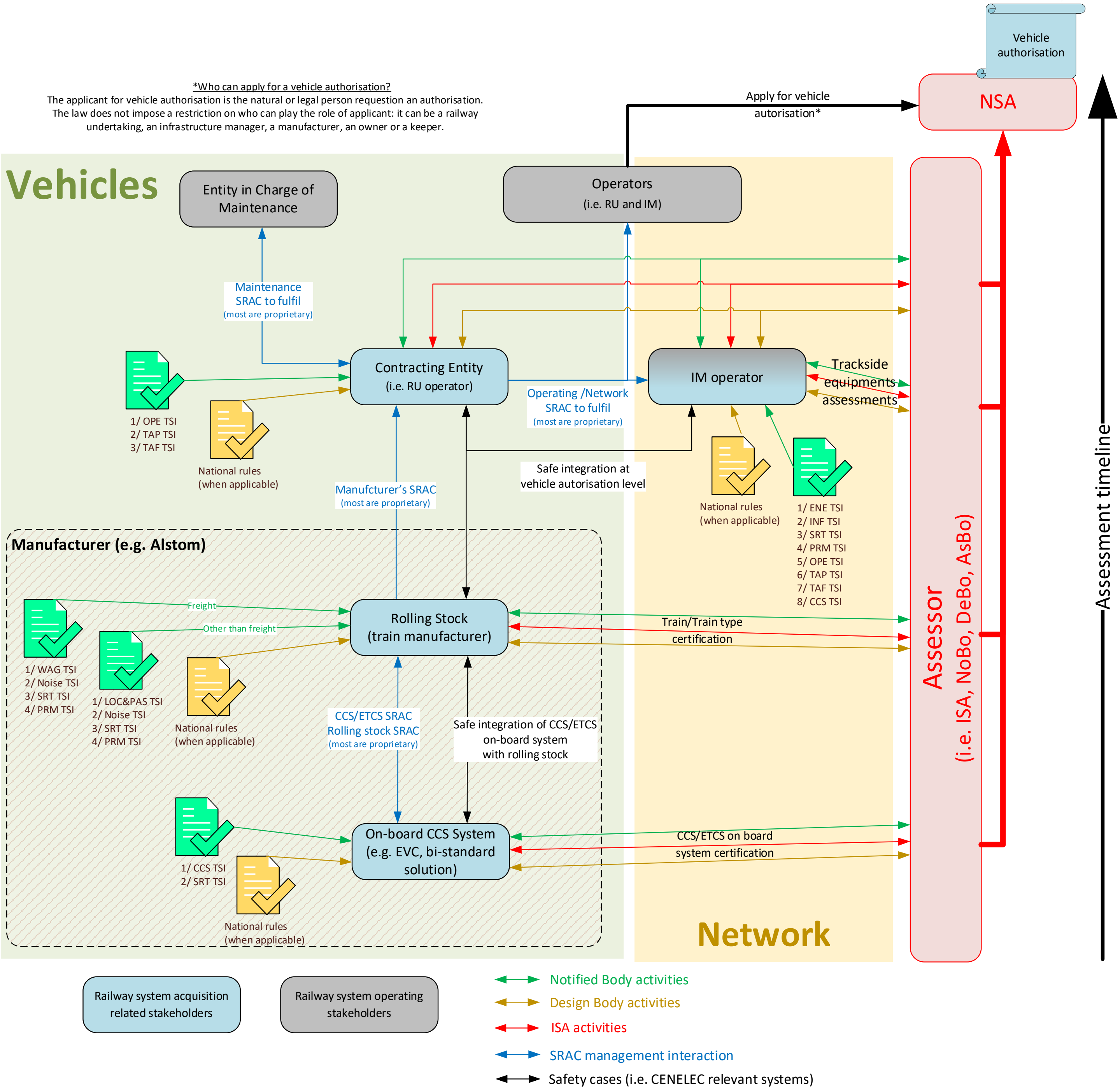

Vehicle authorisation
NSA
Apply for vehicle autorisation*
*Who can apply for a vehicle authorisation?
The applicant for vehicle authorisation is the natural or legal person requestion an authorisation.
The law does not impose a restriction on who can play the role of applicant: it can be a railway undertaking, an infrastructure manager, a manufacturer, an owner or a keeper.
Vehicles
Entity in Charge of Maintenance
Operators (i.e. RU and IM)
Maintenance SRAC to fulfil (most are proprietary)
Contracting Entity (i.e. RU operator)
IM operator
Trackside equipments assessments
Operating /Network SRAC to fulfil (most are proprietary)
1/ OPE TSI
2/ TAP TSI
3/ TAF TSI
National rules (when applicable)
Safe integration at vehicle autorisation level
Manufcturer's SRAC (most are proprietary)
National rules (when applicable)
1/ ENE TSI
2/ INF TSI
3/ SRT TSI
4/ PRM TSI
5/ OPE TSI
6/ TAP TSI
7/ TAF TSI
8/ CCS TSI
Manufacturer (e.g. Alstom)
Freight
Other than freight
Rolling Stock (train manufacturer)
Train/Train type certification
1/ WAG TSI
2/ Noise TSI
3/ SRT TSI
4/ PRM TSI
1/ LOC&PAS TSI
2/ Noise TSI
3/ SRT TSI
4/ PRM TSI
National rules (when applicable)
CCS/ETCS SRAC Rolling stock SRAC (most are proprietary)
Safe integration of CCS/ETCS on-board system with rolling stock
On-board CCS System (e.g. EVC, bi-standard solution)
CCS/ETCS on board system certification
1/ CCS TSI
2/ SRT TSI
National rules (when applicable)
Network
Assessor (i.e. ISA, NoBo, DeBo, AsBo)
Assessment timeline
Railway system acquisition related stakeholders
Railway system operating stakeholders
Notified Body activities
Design Body activities
ISA activities
SRAC management interaction
Safety cases (i.e. CENELEC relevant systems)

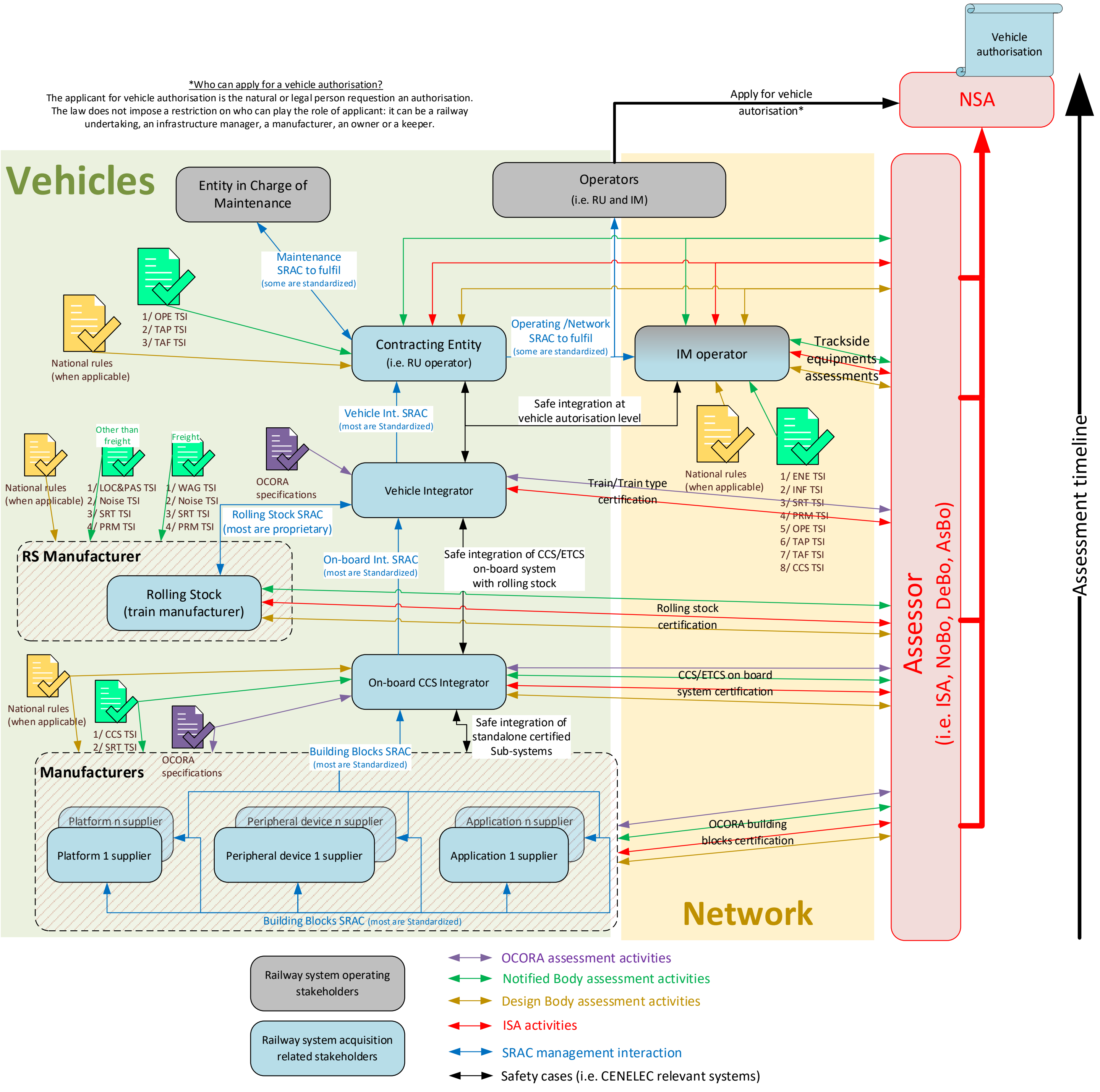
Figure 7 Current ERTMS approval process

Figure 8 tends to present a possible future ERTMS approval that integrates OCORA requirements. **It must be understood that the assignment of the suppliers, CCS-OB integrator, vehicle integrator and system integrator are not defined by OCORA**. Each contracting entity is responsible for assigning these roles to chosen actors. OCORA will focus on the definition of the tasks and responsibilities for them.

Depending on the maturity of the RU regarding technical skills for CCS-OB integration activities, different possibilities can be suggested:

- The first OCORA compliant projects handled by a contracting entity may request these integration activities to historical train manufacturers (e.g. Alstom, Siemens),
- After several successful projects, the contracting entity has developed some skills and knowledge related to safe integration and can now handle these two roles internally.

Again, these are just typical suggestions that may likely occur in the future.



*Who can apply for a vehicle authorisation?
The applicant for vehicle authorisation is the natural or legal person requestion an authorisation.
The law does not impose a restriction on who can play the role of applicant: it can be a railway undertaking, an infrastructure manager, a manufacturer, an owner or a keeper.
Vehicle authorisation
NSA
Apply for vehicle autorisation*
Vehicles
Entity in Charge of Maintenance
Operators (i.e. RU and IM)
Maintenance SRAC to fulfil (some are standardized)
1/ OPE TSI
2/ TAP TSI
3/ TAF TSI
National rules (when applicable)
Contracting Entity (i.e. RU operator)
Operating /Network SRAC to fulfil (some are standardized)
IM operator
Trackside equipments assessments
Vehicle Int. SRAC (most are Standardized)
Safe integration at vehicle autorisation level
National rules (when applicable)
1/ ENE TSI
2/ INF TSI
3/ SRT TSI
4/ PRM TSI
5/ OPE TSI
6/ TAP TSI
7/ TAF TSI
8/ CCS TSI
Other than freight
Freight
National rules (when applicable)
1/ LOC&PAS TSI
2/ Noise TSI
3/ SRT TSI
4/ PRM TSI
1/ WAG TSI
2/ Noise TSI
3/ SRT TSI
4/ PRM TSI
OCORA specifications
Vehicle Integrator
Train/Train type certification
Rolling Stock SRAC (most are proprietary)
RS Manufacturer
Rolling Stock (train manufacturer)
On-board Int. SRAC (most are Standardized)
Safe integration of CCS/ETCS on-board system with rolling stock
Rolling stock certification
National rules (when applicable)
1/ CCS TSI
2/ SRT TSI
OCORA specifications
On-board CCS Integrator
CCS/ETCS on board system certification
Safe integration of standalone certified Sub-systems
Building Blocks SRAC (most are Standardized)
Manufacturers
Platform n supplier
Platform 1 supplier
Peripheral device n supplier
Peripheral device 1 supplier
Application n supplier
Application 1 supplier
OCORA building blocks certification
Building Blocks SRAC (most are Standardized)
Network
Assessor (i.e. ISA, NoBo, DeBo, AsBo)
Assessment timeline
Railway system operating stakeholders
Railway system acquisition related stakeholders
OCORA assessment activities
Notified Body assessment activities
Design Body assessment activities
ISA activities
SRAC management interaction
Safety cases (i.e. CENELEC relevant systems)

Figure 8 ERTMS approval process including OCORA

The complete decomposition of the two above pictures will be done in another document that will be started in future release of OCORA. The main task is to define the activities handled by the three integrators' steps. Their scopes of activities have to be defined for:

- First realization of an OCORA compliant CCS-OB (e.g. retrofit of an existing vehicle) and then,
- Evolution of the OCORA compliant CCS-OB once certified.

The first bullet will be addressed in another document whereas the second in the current document.

In both cases, the key point to be followed is that the two kinds of integrators must realize safe integration.

The latter, detailed in Directive 2018/545 [23], warns the different stakeholders about the wrongly understood limit of safe integration:

2.5.6. In general, the stakeholders responsible for changes of the design of the railway system, i.e. the infrastructure managers and railway undertakings, each one for its part of the system, ***cannot thus be satisfied only with*** *:*

(a) cutting the overall system into a list of constituting sub-systems.

(b) waiting for the suppliers to develop the different sub-systems and then just putting them together technically.

(c) collecting the bottom-up exported safety related application conditions/constraints (SRACs) from the different constituting sub-systems/suppliers.

(d) demonstrating the compliance with those safety related application conditions/constraints imported from the risk assessment of every constituting sub-system/involved actor.

2.5.7. They must consider also the potential impacts of the considered change on:

(a) the other unchanged elements, components, constituents, structural or functional sub-systems of the railway system.

(b) the interfaces with those other elements, components, constituents of the railway system.

2.5.8. In addition to the routine changes of the railway system, there could be other types of changes that are not driven directly by a railway undertaking or an infrastructure manager. Typical examples are:

(a) a financial consortium, or a regional public authority, which purchases a fleet of vehicles or trains from a manufacturer without consulting and involving the future railway undertaking(s), who will operate the vehicles, and the infrastructure manager on whose lines the vehicles will operate.

(b) a regional public authority, or the Ministry, purchases the construction of a new, or the extension of an existing, (regional) railway line to a contractor without involving the infrastructure manager who will manage the traffic on the line.

In order to manage properly these types of changes, and to improve the hazard identification and the proper preventive control of the associated risks, it is essential that the “procurement entity” also applies the top-down and system-based approach described in this paper. Right from the tender stage, and from the beginning of the project, the procurement entity should either involve the future operators (RUs) and the traffic manager (IM) in, or sub-contract to them, the proper management of the project. This gives the possibility to systematically identify early in the project the potential risks and to control the identified risks through technical improvements of the design instead of obliging the users to implement afterwards constraining operational and maintenance safety related application conditions for use.

2.5.9. In the absence of top-down system risk assessment and system risk management, some railway system hazards/risks might be non-identified and the associated system risk control measures missing. The proper risk assessments and risk managements of the constituting sub-systems cannot compensate the lack of proper risk identification and risk control at the level of the railway system.

Following that, ERA 1209-063 Clarification note on safe integration [24] presents the strategy to handle a safe integration when dealing with evolutions in one part of the overall vehicle authorization process. The following activities have been identified:

1) *Whenever a new element is introduced into a system, or an existing one is modified, regardless of significance, safe integration and risk management must ensure that:*

a) the new or modified element is technically compatible, and thus correctly interfaces, with the other parts of the system into which it is introduced.

b) the new or modified element is safely designed and fulfils all the intended functional and technical objectives.

c) the impacts of humans on the operation and maintenance of that element and on the system where it is incorporated are assessed and properly addressed.

d) the introduction of that new or modified element into its physical, functional, environmental, operational *and maintenance context does not have adverse and unacceptable effects on safety of resulting system into which it is incorporated*

Therefore, every actor is responsible for the risk assessment and the safe integration of its contributing part to the overall railway system

2) *Safe integration of a change is therefore not a separate and additional set of tasks to the regular risk assessment and risk management activities.*

The above elements must be taken in account when developing the integration of evolved OCORA compliant systems.

2.7 ISA activities for OCORA evolved systems

Assessment activities use to represent a significative cost of the overall SuC evolution. Therefore, it is a challenge to identify the cases when a new assessment is required and when it can be avoided without degrading the overall safety target of the SuC.

The management of evolutions during the CCS-OB and its constituents' lifetime is introduced by the CENELEC standards.

EN 50129 [17] states:

> *8.3 Modification and retrofit*
>
> *During the operational life of a system, change requests can be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation.*
>
> *Where a change request results in a modification which could affect the safety of the system, or associated systems, or the environment, the appropriate portion of the safety life cycle shall be repeated to ensure that the implemented modification does not unacceptably reduce the level of safety.*
>
> *Modifications shall be controlled using the same quality management, safety management and functional/technical safety criteria as would be used for a new design. All relevant documentation, including the Safety Case, shall be updated **or supplemented by additional documentation**.*

In addition, EN 50506-2 [20] provides more context data on evolutions assessments:

> *6.3.1 Conditions*
>
> *General conditions for any system change:*
>
> - *the rationale for any change should be documented in a change request;*
> - ***any change should result in a new revision/version of the equipment;***
> - *any change should be subject to a documented change management process, which should include a safety impact analysis;*
>
> *In simple cases (internal adaptation of the component) **the approval by the safety authority of the modification of already approved equipment with electronic components can be dispensed** with if*
>
> - *no new Hazards have been introduced (Hazard Analysis has not changed), and*
> - *the Technical Safety Report remains unchanged, and*
> - *the required function of the electronic component is not changed by the adaptation (no modification of specification), and*
> - *the interfaces of the electronic component remain unchanged, and*
> - *an assessment without objections has been carried out by an approved/accredited assessor.*

Today, there is struggle when deploying this modifications process in into GPSC or GASC development. Indeed, the Safety Case of the SuC shall present its product breakdown structure with the version of all components (e.g. Hw boards, Sw executable files). This concerns both safe and non-safe parts of the SuC. Based on that, when such an element evolves, its global version must be increased (as defined by 6.3.1 condition above) which finally leads to an updated of the whole SuC and therefore an update of the Safety Case. From that, a new assessment is expected as the latter was updated too. This struggle is even more important when SuC design is not segregated between safe and non-safe parts.

Based on the previous statement, OCORA compliant systems could benefit from the modular architecture to integrate improvements in the way to handle the assessments of evolved systems.

The background of safety managers composing the OCORA RAMS team show that already today, some industry suppliers have defined granular assessments in their proprietary modular systems.

Four levels of assessments have been identified and could be deployed in this evolution management, in respect with the safety regulations and without degrading the overall safety level:

- **No ISA activities**: this is the typical example presented in the EN 50506-2 [20] criteria above,
- **Yearly letter of support**: this type of assessment can be used only:
    - At building block level: when an evolution of a non-safe part of a segregated SuC occurs without impact on the safe partition,
    - At CCS-OB level: when an evolution of one or several non-safe building blocks occurs.

  The activities consist for the supplier or the CCS integrator to follow his internal quality management process to handle the modification, save it in its records, increase the version of the SuC as a minor version and present once a year this evolution report to the ISA so that the last valid ISA certificate can be amended with all the minor versions produced during the year.

  The complete frame of the definition and use of such type of assessment will be defined in detailed in a later release of OCORA with the support of ISAs.
- **Letter of support:** this type of assessment aims at covering minor modifications. The quantification of “minor” is the purpose of the significance matrix defined in section 3. The letter of support represents an assessment focusing on the evolution itself in the SuC without rechallenging the already certified parts and thus, without impacting the last valid “technical report” presented in the safety case. It is represented by the “***supplemented by additional documentation***” mentioned by EN 50129 [17] extract above.

  The complete frame of the use of such type of assessment will be defined in detailed in a later release of OCORA with the support of ISAs.
- **New assessment:** this is the usual way of handling evolution when the conditions presented in the EN 50506-2 [20] criteria above are not met.

3 Significance process and matrix

As presented on Figure 6, the first main task of the OCORA RAMS team is to define the significance matrix used to determine which level of assessment is recommended for the current evolution. The same figure shows that several iterations of the evolution management process are required from building block level to system level. The present version of the significance process focuses on the building block evolutions that represents the core of OCORA and where this process will have the most impact. The other iterations (i.e. CCS-OB, vehicle and system) will be developed in a future release of the document.

The significance matrix process is defined according to 8 steps presented on Figure 9. Some of them are allocated to the SuC Design team (e.g. System architect, Sw designer) and other to the SuC safety manager.

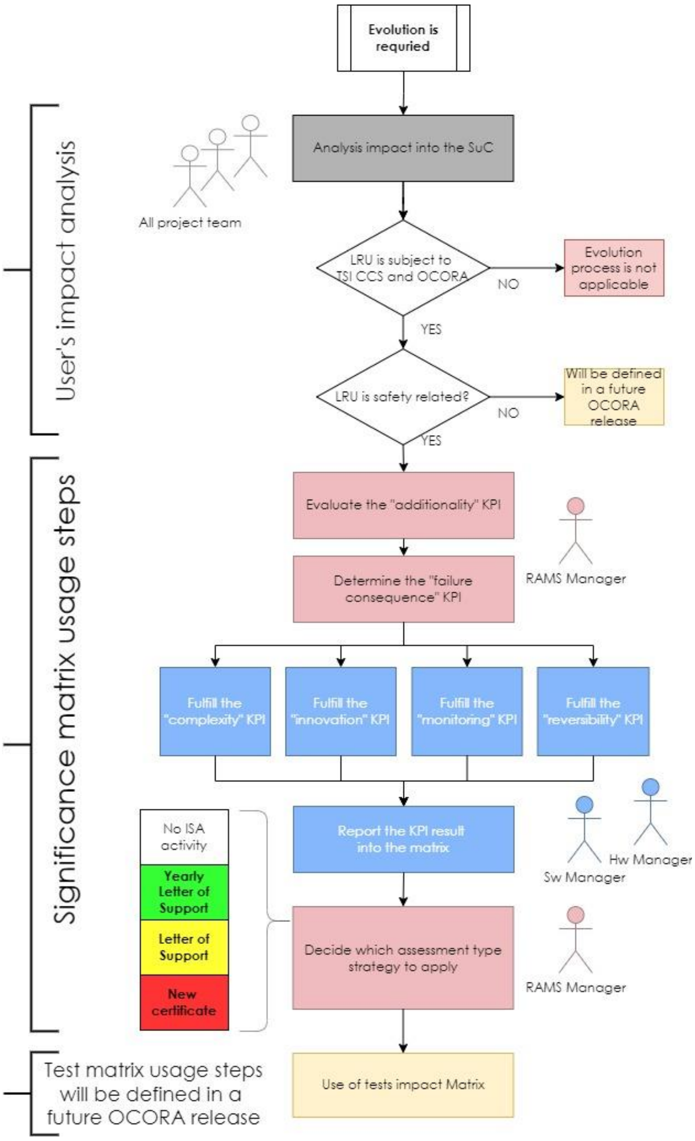

Evolution is requried
Analysis impact into the SuC
All project team
User's impact analysis
LRU is subject to TSI CCS and OCORA
NO
Evolution process is not applicable
YES
LRU is safety related?
NO
Will be defined in a future OCORA release
YES
Significance matrix usage steps
Evaluate the "additionality" KPI
RAMS Manager
Determine the "failure consequence" KPI
Fulfill the "complexity" KPI
Fulfill the "innovation" KPI
Fulfill the "monitoring" KPI
Fulfill the "reversibility" KPI
No ISA activity
Yearly Letter of Support
Letter of Support
New certificate
Report the KPI result into the matrix
Sw Manager
Hw Manager
Decide which assessment type strategy to apply
RAMS Manager
Test matrix usage steps will be defined in a future OCORA release
Use of tests impact Matrix

Figure 9 Significance process for the building blocks evolution

The current process aims at covering any type of evolution impacting an OCORA compliant system through its lifetime and the lifetime of the overall system where it is used (see Figure 13 for illustration).

The process starts when the SuC project team (e.g. architects, designers, safety managers) has performed the impact analysis of the evolution and determine if the OCORA evolution management process can be applied on the SuC. Up to release R2 of OCORA this process only covers safety relevant systems compliant to OCORA. In a further release of OCORA, it will be extended to non-safe systems compliant to OCORA.

The first criterion defined in CSM-RA [22] to be considered by the SuC safety manager is the *additionality* which is defined as follow:

> *(f) additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.*

In the context of OCORA, the additionality consists in analyzing the gap between the last valid ISA certificate and the current situation. This means checking the number and purpose of the letter of support (if any) emitted for the SuC. A maximum number plus additional conditions should be fixed by any supplier which could lead, once, reached to realize again a complete re-assessment for the system, whatever the evolution relies on.

The second criterion defined in CSM-RA [22] to be considered by the SuC safety manager is the *failure consequence* which is defined as follow:

> *(a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;*

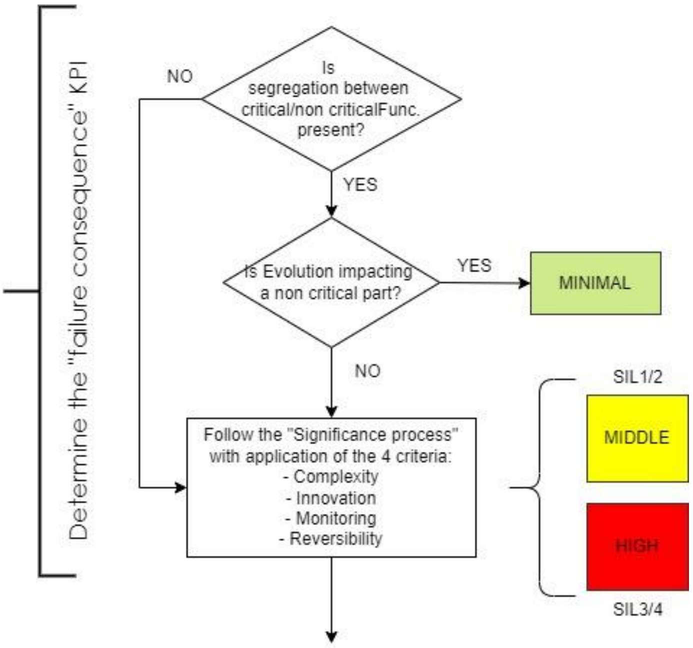
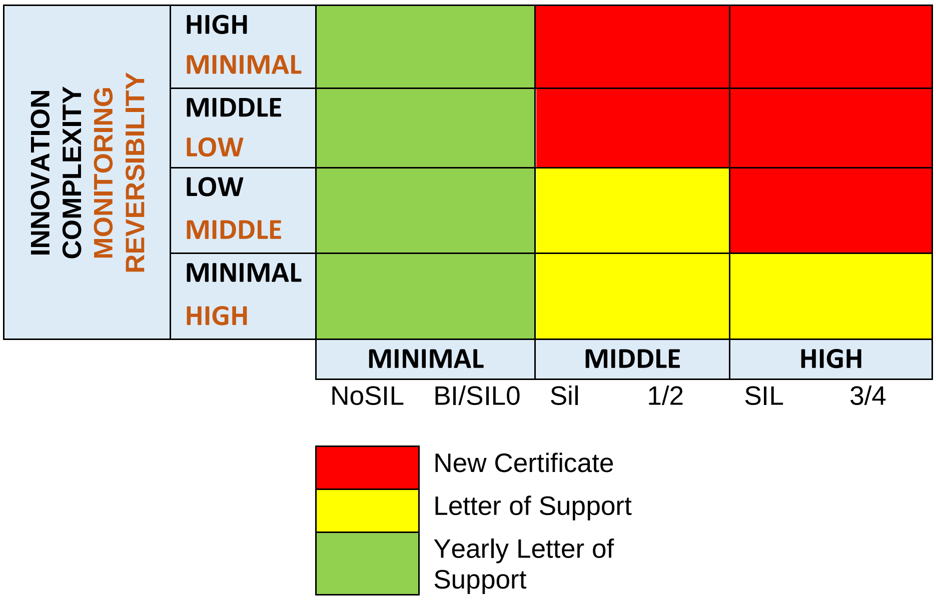

Determine the "failure consequence" KPI
NO
Is segregation between critical/non criticalFunc. present?
YES
Is Evolution impacting a non critical part?
YES
MINIMAL
NO
Follow the "Significance process" with application of the 4 criteria:
- Complexity
- Innovation
- Monitoring
- Reversibility
SIL1/2
MIDDLE
HIGH
SIL3/4

Figure 10 Failure consequence sub-process

In the OCORA context, the failure consequence is defining based on 3 questions:

- Is the SuC safety related? In case the answer is “no”, the current process is not applicable in its current version.
- Is segregation between critical and non-critical functions implemented? In the context of OCORA “critical” likely refers to safety but in the future, it could also concern RAM functions depending of the SuC under consideration. In case the answer is “no”, the user has to consider the additional KPI of the process defined on Figure 9.
- Is the evolution impacting a non-critical part? This is relevant only for segregated systems between safe and non-safe parts and later also between other types of segregations (e.g. RAM, cybersecurity).
  - To answer “yes”, the impact analysis performed by the user must show that no impacted requirements is traced with a SuC hazard. The failure consequence is then categorized as “MINIMAL” in the significance matrix in Figure 11, (i.e. first column is selected) and then, only a yearly letter of support is recommended for the evolution’s assessment.
  - If the answer is “no”, then the user has to consider the additional KPI of the process defined on Figure 9.

When the answers to these questions are known, the user can select the column to use for the failure consequence before continuing the evolution process.



INNOVATION COMPLEXITY MONITORING REVERSIBILITY				
	HIGH MINIMAL	🟩	🟥	🟥
	MIDDLE LOW	🟩	🟥	🟥
	LOW MIDDLE	🟩	🟨	🟥
	MINIMAL HIGH	🟩	🟨	🟨
		MINIMAL NoSIL BI/SIL0	MIDDLE Sil 1/2	HIGH SIL 3/4

🟥	New Certificate
🟨	Letter of Support
🟩	Yearly Letter of Support

Figure 11 Significance matrix

The following criteria aim at choosing the line in the matrix (see Figure 11) from “MINIMAL” to “HIGH”.

The third criterion defined in CSM-RA [22] to be considered by the SuC designers is the *innovation/novelty* which is defined as follow:

> *(b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organization implementing the change;*

In the OCORA context, the innovation is proposed to be determined thanks to the same criteria as the Swiss national regulation RTE 49100 [25], adapted to the OCORA environment:

- a) technical code of practice (e.g. norms, directives) can be used to realize the evolution?
- b) the evolution has already been successfully deployed and no critical failure of the evolution has been detected so far on similar products/system in commercial revenue?
- c) the evolution remains in the actual state of technique (e.g. FRMCS, ATO GoA 3/4 are beyond actual scope)?

  Note: competitors have similar products already on the market"
- d) The evolution corresponds to the reference system defined by TSI CCS 2016 (and when applicable 2022)?

The answer to these questions can later be used as follow in the significance matrix (see Figure 11):

- 0 answer is NO: complexity is judged as “MINIMAL”,
- 1 answer is NO: complexity is judged as “LOW”,
- 2 answers are NO: complexity is judged as “MEDIUM”,
- 3 or 4 answers are NO: complexity is judged as “HIGH”,

The fourth criteria defined in CSM-RA [22] to be considered by the SuC designers is the *complexity* which is not properly defined as it is unambiguous.

In the OCORA context this criterion is the most difficult to quantify. Generic metrics cannot be defined by OCORA; it is under the responsibility of each user to define its own complexity metrics to be deploy in his company.

Nevertheless, the OCORA initiative proposes a list of technical items that must be taken in account when defining the complexity of an evolution (only as informative):

- Software:
  - What is the context of the evolution; improvement of existing function, bug fixing, patch for safety issue,
  - How big is the modification; how many source code lines, functions, modules are modified,
  - Difficult understanding of the evolution (i.e. technical point of view): YES/NO,
- Technical file (i.e. documentation used to build the technical safety report presented in the safety case): How many technical documents must be modified?
- Mechanical: is there an impact on the mounting parts, weight of the SuC, connectors, rack…,
- Electrical: is there an impact on simple components such as fans, horns, on more complex components, EMC filters, power supplies,
- Installation, commissioning and maintenance: are there new SRAC/AC linked to the evolution? How many changes are there for the user (e.g. new procedure for maintenance, new tool required).

The fifth criterion defined in CSM-RA [22] to be considered by the SuC designers is the *monitoring* which is defined as follow:

> *(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;*

In the OCORA context, this refers to the inability for a SuC to monitor its own behavior or being monitored by a third system. Usually, this is covered by self-testing; at start-up and/or during operation. The more this monitoring is accurate and frequent, the more this criterion can be considered as important. Different shades can be considered such as:

- Continuous self-test of the evolved function (e.g. every hour) with information to the related supervisor (e.g. driver, ATP): it can be considered as “HIGH”,
- Self-test performed during periodic maintenance inspection; the defect can be identified only in workshop: it can be considered as “MIDDLE”,
- Defect can be detected during periodic maintenance inspection: it can be considered as “LOW”,
- No detection at all, the SuC has to be sent back to the supplier for deeper investigation: no on-site maintenance, it can be considered as “MINIMAL”.

The last criterion defined in CSM-RA [22] to be considered by the SuC designers is the *reversibility* which is defined as follow:

> *(e) reversibility: the inability to revert to the system before the change;*

In the OCORA context, this refers to the retrofit of the SuC into a previous certified version. Here are some examples to help at defining the granularity of the reversibility:

- The retrofit to a previous version is not possible. It requires the replacement of the complete LRU (e.g. Hw redesign): reversibility can be considered as “MINIMAL”,
- The retrofit to a previous version requires to send the SuC back to the supplier (e.g. Hw internal board replacement): reversibility can be considered as “LOW”,
- The retrofit to a previous version requires to physically be connected to the LRU after a trip journey (e.g. manual Software downgrade). This must be done SuC per SuC: reversibility can be considered as “MIDDLE”,
- The retrofit to a previous version can be done remotely after a trip journey (e.g. automatic Software downgrade). This can be done on an entire SuC fleet in a one shot: reversibility can be considered as “HIGH”.

When all criteria have been quantified, their values can be reported in the significance matrix (see Figure 11) by the SuC designers. There are different possibilities to combine these criteria together to finally status on the “horizontal” side of the matrix. EN 17023 [19] provides two other examples of combinations:

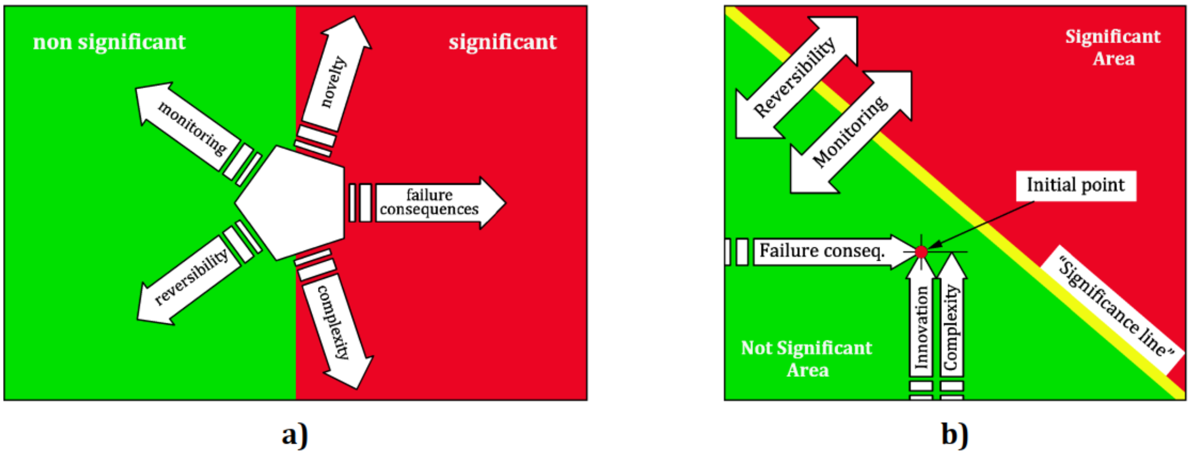


Figure 12 Diagram of Safety Significance Analysis from EN 17023 [19]

In OCORA context, the matrix presented on Figure 11 is proposed because it seems easier to deploy than other examples from EN 17023 [19]. Thus, each process user is free to choose the configuration that suits him the best. A general rule must be respected by the evolution process users; *complexity* and *innovation/novelty* have must have a stronger weight than *monitoring* and *reversibility*. Indeed, it is obvious that an evolution classified as HIGH in all four criteria cannot be considered as “non-significant without assessment” or “non-significant with letter of support”, considering that the 4 criteria are balancing each other’s.

A proposition of combination of the four criteria into the matrix will be provide in the next release of the document.

Based on the result of the six criteria and their weight, each RAMS manager is able to identify with a systematic approach the most relevant assessment strategy to be used to develop the SuC’s evolution.

This evolution management process will be shared with a panel of assessors to ensure that the overall strategy is valid for an individual implantation by any supplier or integrator.

Each process user has then the responsibility to develop his own quantification metrics for each criterion and submit them to his assessor before using it in his OCORA compliant system development.

4 Test impact process and matrix

The second major step of the overall evolution management process represents the management of the testing activities focusing on OCORA interfaces. This has been introduced in the OCORA Testing Strategy [11] and is further developed in the present section.

It must be noticed that up to R2, only high-level discussions have been performed. The detailed activities, meaning the definition of non-regression scope of tests for each level will be performed in a further release of OCORA where the technical requirements for the different building blocks will be available.

Figure 13 represents all different kind of high-level cases to be handled during the CCS-OB lifetime. In its top horizontal is represented the lifetime of the CCS-OB system made of different OCORA compliant building blocks. On the latter are presented the different evolution types that can occur through the years.

The red color on the different connections on Figure 13 presents the focus of testing activities, depending on the SuC under evolution.

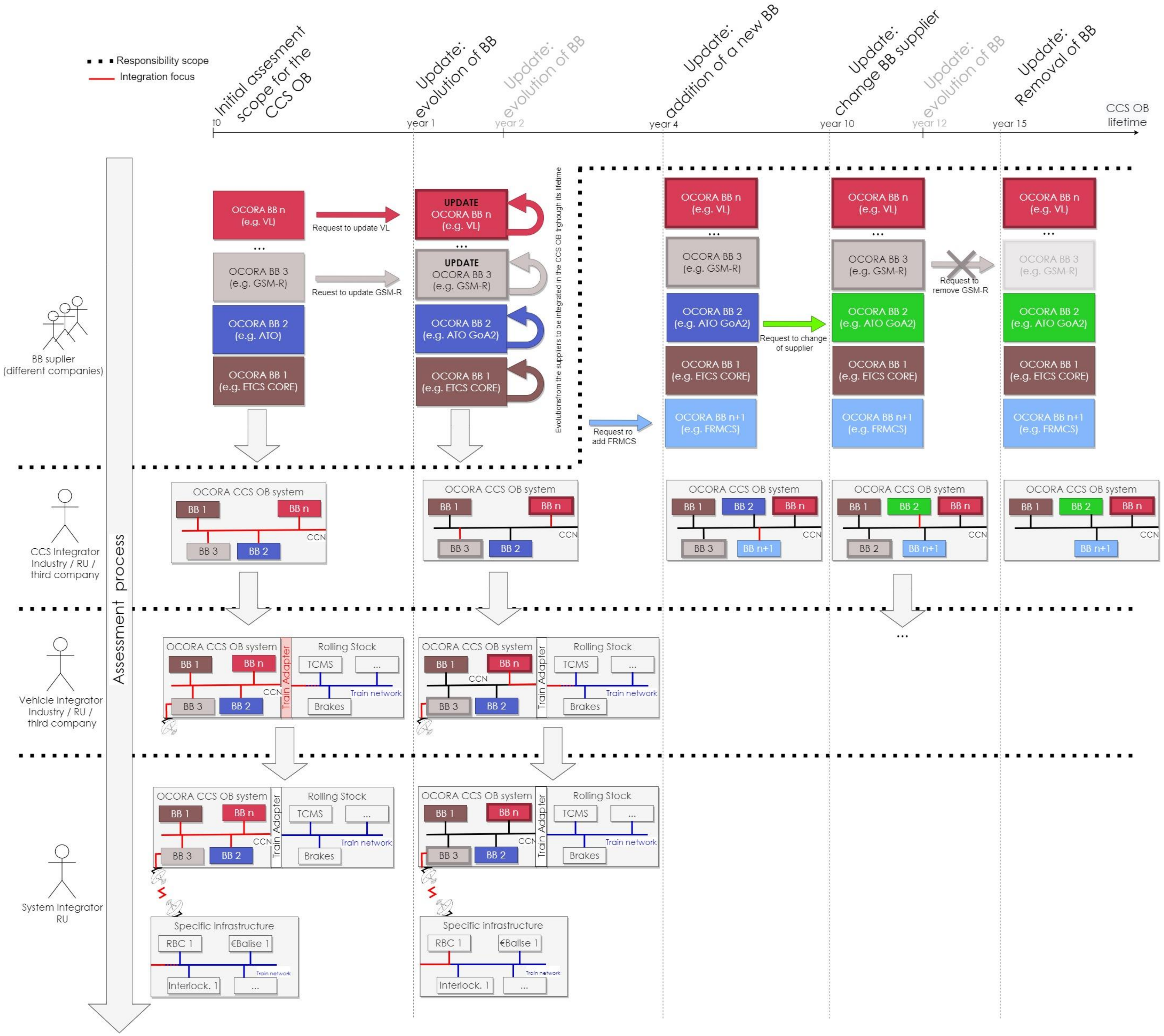


Figure 13 Overall evolution process representation

4.1 First delivery of the CCS on board system

This is the very first step of the CCS-OB lifetime. For the building blocks suppliers, it represents the realization of their systems according to the applicable regulation defined in section 2.4.1 and their assessment.

At this step, the full scope of test at building block level will be mandatory. These are represented by levels 0, 1 and 2 in the OCORA Testing Strategy [11].

When the building blocks are available on the market, they must be safely integrated into a CCS-OB system as presented in section 2.6.

Again, the CCS-OB integrator has to perform the full scope of tests defined at this level by the testing team (refer to level 3 in the OCORA Testing Strategy [11]). This kind of tests focus on the integration of the building blocks used as “black-box” by the CCS-OB integrator.

The CCS-OB integrator (i.e. the role name in this document represents a team of different skilled people) is responsible to perform these tests, create the GASC and manage its assessment according to the applicable regulation defined in section 2.4.1.

When the generic CCS-OB system is certified and ready for deployment, it will then be integrated into one (or several) train types and seen as a “black box” by the vehicle integrator.

At this level the focus is done in its integration with the rolling stock through the Train Adapter building block. The latter aims at using a same generic CCS-OB in different train type holding different legacy train networks (e.g. CAN, MVB, Ethernet). As this is the first integration CCS-OB into a vehicle, the full scope of tests defined at this level by the testing team (refer to level 4 in the OCORA Testing Strategy [11]) is applicable.

The vehicle integrator is responsible to perform these tests, create the GASC and manage its assessment according to the applicable regulation defined in section 2.4.1 and in the Optimized Approval Process [12]. The strategy on the reuse of the first vehicle type on additional fleet is covered by the Optimized Approval Process [12].

As soon as the vehicle is authorized, it can be integrated on an authorized network by the system integrator into a specific application.

At this level, the focus is done on the interconnection between the building blocks (when applicable) and the trackside world (e.g. GSM-R, Eurobalises). As this is the first integration of this kind of vehicle into the network, the full scope of test defined at this level by the testing team (refer to level 5 in the OCORA Testing Strategy [11]) is applicable.

The system integrator is responsible to perform these tests, create the SASC and manage its assessment according to the applicable regulation defined in section 2.4.1 and in the Optimized Approval Process [12]. This ends with the first Authorization for Placing on the Market document as required by [23] and developed in the Optimized Approval Process [12].

4.2 Update of building blocks

After the first years of the CCS-OB assessment, the first evolutions of its building blocks will be available. This is the first kind, and likely most common, evolution type which will occur regularly during the CCS-OB lifetime. This is shown on Figure 13 with the different occurrences of “update: evolution of BB”.

First, the supplier of the evolved building block has to apply the significance process presented in section 3 to determine the assessment strategy to apply. Then, he must use the test impact matrix (will be published in a future release of OCORA) and realize the corresponding non-regression scope of tests plus the ones focusing on the evolution itself (under the user’s responsibility).

When the new version of the building block has been re-assessed (if necessary) and is ready for commercial revenue, the CCS-OB integrator can install it in the existing system. He has to apply at his level the significance process presented in section 3 to determine which assessment strategy is relevant. Obviously, the criteria quantification metrics differ from the ones proposed by OCORA in section 3 and must focus on the evolution's potential impact on OCORA standardized interfaces (i.e. black-box vision).

Therefore, the question to be answered by the CCS-OB integrator is: *"is the evolution of the building block having an impact on one or several CCS-OB OCORA standardized interfaces (the detailed list will be proposed in a future release of the document)?"*

If the answer is "yes", then the full scope of tests related to the building block integration has to be performed again.

If the answer is "no", then only the generic scope of non-regression tests is required for the safe integration.

The answer to that question will directly impact the assessment level for the evolved CCS-OB. This will be developed in a future release of the document.

The same strategy applies then at vehicle first and finally at system level where the focus is done on:

- Impacted OCORA standardized interface(s) with rolling stock (e.g. SCI-FVA interface as defined in OCORA System Architecture [8]) for the vehicle integrator,
- Impacted OCORA standardized interface(s) with the network (e.g. PI-VLS interface as defined in OCORA System Architecture [8]) for the system integrator,

For the vehicle and system levels, the current evolution management process has to be deployed first and completed by the use of the Optimized Approval Process [12] (see Figure 6) for the management of the European authorizations defined by [23].

4.3 Addition of a new building block in the CCS-OB

This kind of evolution will occur mainly to introduce the future game changers. It starts at CCS-OB level as it is assumed that the building block has been developed according to the conditions presented in section 4.1.

From CCS-OB level to the system one, this building block has to be handled as new element, meaning the full scope of integrated tests has to be performed. In that case, at CCS-OB level, the significance matrix will lead to request a new assessment, assuming that the building block is safety related.

For vehicle and system level, the following question must be answered:

- For the vehicle integrator; is the new building block impacting an OCORA standardized interface(s) with rolling stock (e.g. SCI-FVA interface as defined in OCORA System Architecture [8])?
- For the system integrator; is the new building block impacting an OCORA standardized interface(s) with the network (e.g. PI-VLS interface as defined in OCORA System Architecture [8])?

Depending on the answer, the assessment strategy will differ. This will be developed in a future release of the document.

4.4 Removal of a building block in the CCS-OB

This kind of evolution will occur when a CCS-OB integrator wants to remove a building block realizing functions that are no more used in the current version of the TSI CCS (e.g. GSM-R in several years).

The strategy to be deployed to manage such cases has not been defined yet. This will be developed in a future release. The scope of test will be very limited maybe none, but several questions have to be answered first (not exhaustive for R2):

- Is the building block replacing the one under removal already successfully and safely integrated in the CCS-OB system?
- What happens if an equipment using one removed function tries to communicate with the CCS-OB system?

Depending on the answer, the assessment strategy will differ. This will be developed in a future release of the document.