OCORA

Open CCS On-board Reference Architecture

RAMS – Evolution Management

Document ID: OCORA-TWS07-020

Version: 3.40

Date: 01.12.2022

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 for R2	JB	09.06.2022
3.00	First draft for OCORA R3	JS	29.07.2022
3.10	Update to present configuration management	JB	02.11.2022
3.20	Update before TWS07 review	JS / JB	10.11.2022
3.30	Update following TWS07 comments	JB	18.11.2022
3.40	Final version for R3	JB	01.12.2022

Table of contents

Table of figures

References

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

[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-TWS07-040 - Optimized Approval Process

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

[13] OCORA-TWS09-010_Testing-Strategy

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

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

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

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

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

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

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

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— Communication, signalling and processing systems — Application guide for EN 50129 - Part 2: Safety assurance - withdrawn standard

[22] 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

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

[24] 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

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

[26] 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 5). This topic was 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 evolutions on building blocks and on the integrated CCS OB system. Modifications performed at vehicle and overall system level (i.e. up to the final vehicle authorisation as defined in Directive 2018/545 [24]) are introduced here but managed in the Optimized Approval Process document [11]. This document provides 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 R3, 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 R3 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.

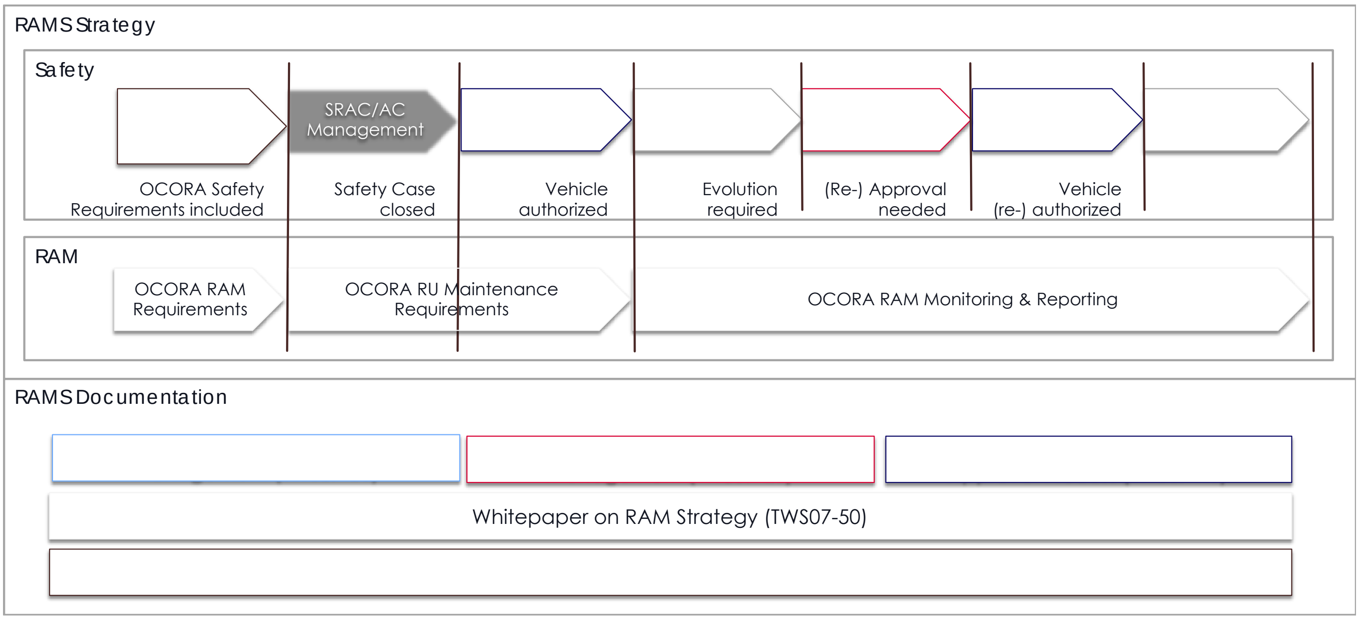


Figure 1 OCORA RAMS Strategy and RAMS Documentation

2 Context of Evolution management

2.1 Current situation regarding CCS OB evolutions

Railway products or systems typically 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 [14]) 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 related systems in the ERTMS environment (e.g. CCS OB) have to be defined according to the TSI CCS [22]. This considers the technical requirements defined by the different SUBSETS and the CENELEC standards (i.e. EN 50126 [14], EN 50128 [16] [for the CCS OB], EN 50657 [17] [for the Train Adapter] and EN 50129 [18]) plus all the additional standards referred in these three main ones (e.g. EN 50159 [19]).

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 [18] 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 for this reason 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 is 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 is worth it from a business point of view and especially from certification point of view (as explained above).

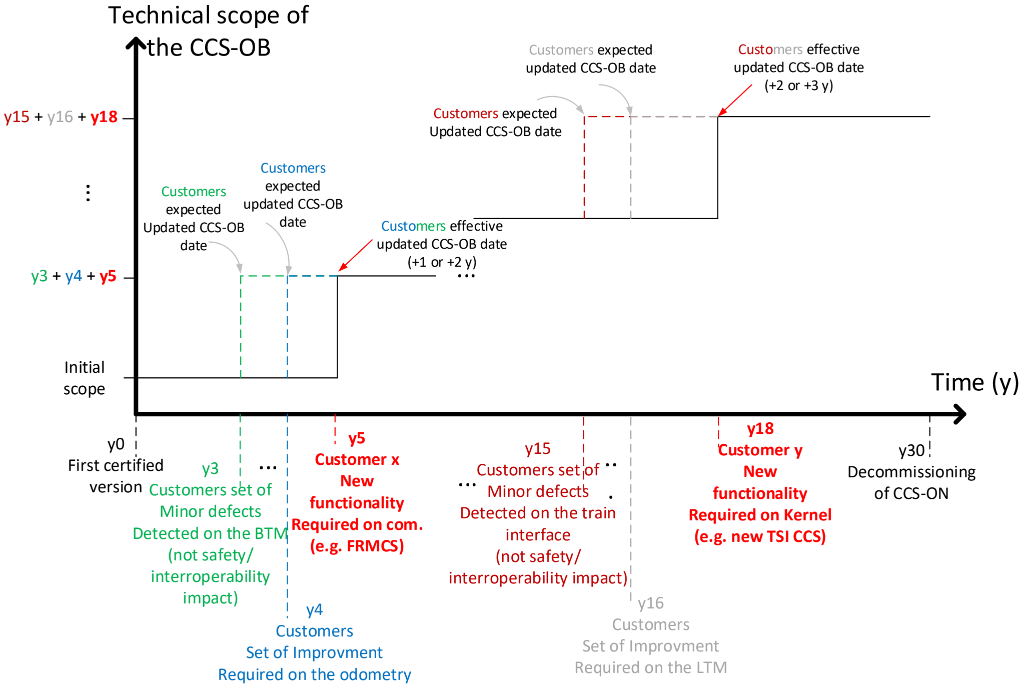
Whatever the scope of the assessment is, the “entry ticket” uses to be high because of preparation of documents, involvement of the assessor in preliminary meetings, documentation to be shared… This directly increases the cost of the “small” evolutions presented above for the customers and most of the 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 conditions required to update the current CCS OB system without delays are when:

- new functionalities are requested (e.g. implementation of SUBSET-119 for TSI 2022) and obviously will be presented 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).

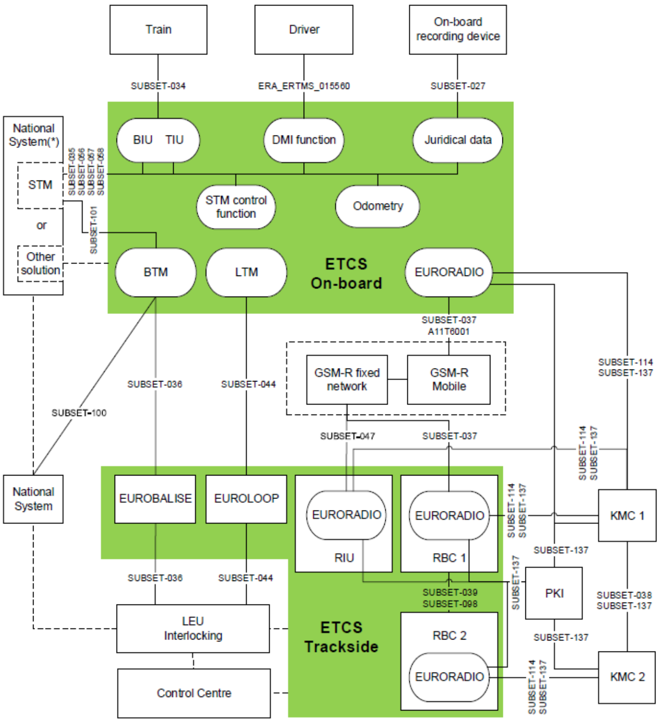
Beside these two cases, the customers use to wait months or even years before having their other change requests integrated into a new version of the CCS OB system.

An additional reason of this “big steps” approach when managing evolutions is that current CCS OB is mostly driven by the ETCS On-board (SUBSET-026 architecture as presented on 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.



Technical scope of the CCS-OB
y15 + y16 + y18
⋮
y3 + y4 + y5
Initial scope
Time (y)
Customers expected updated CCS-OB date
Customers effective updated CCS-OB date (+2 or +3 y)
Customers expected Updated CCS-OB date
Customers expected updated CCS-OB date
Customers expected Updated CCS-OB date
Customers effective updated CCS-OB date (+1 or +2 y)
…
y0 First certified version
y3 Customers set of Minor defects Detected on the BTM (not safety/ interoperability 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/ interoperability 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



(*) 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 [24]. 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 small incremental 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 related 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.

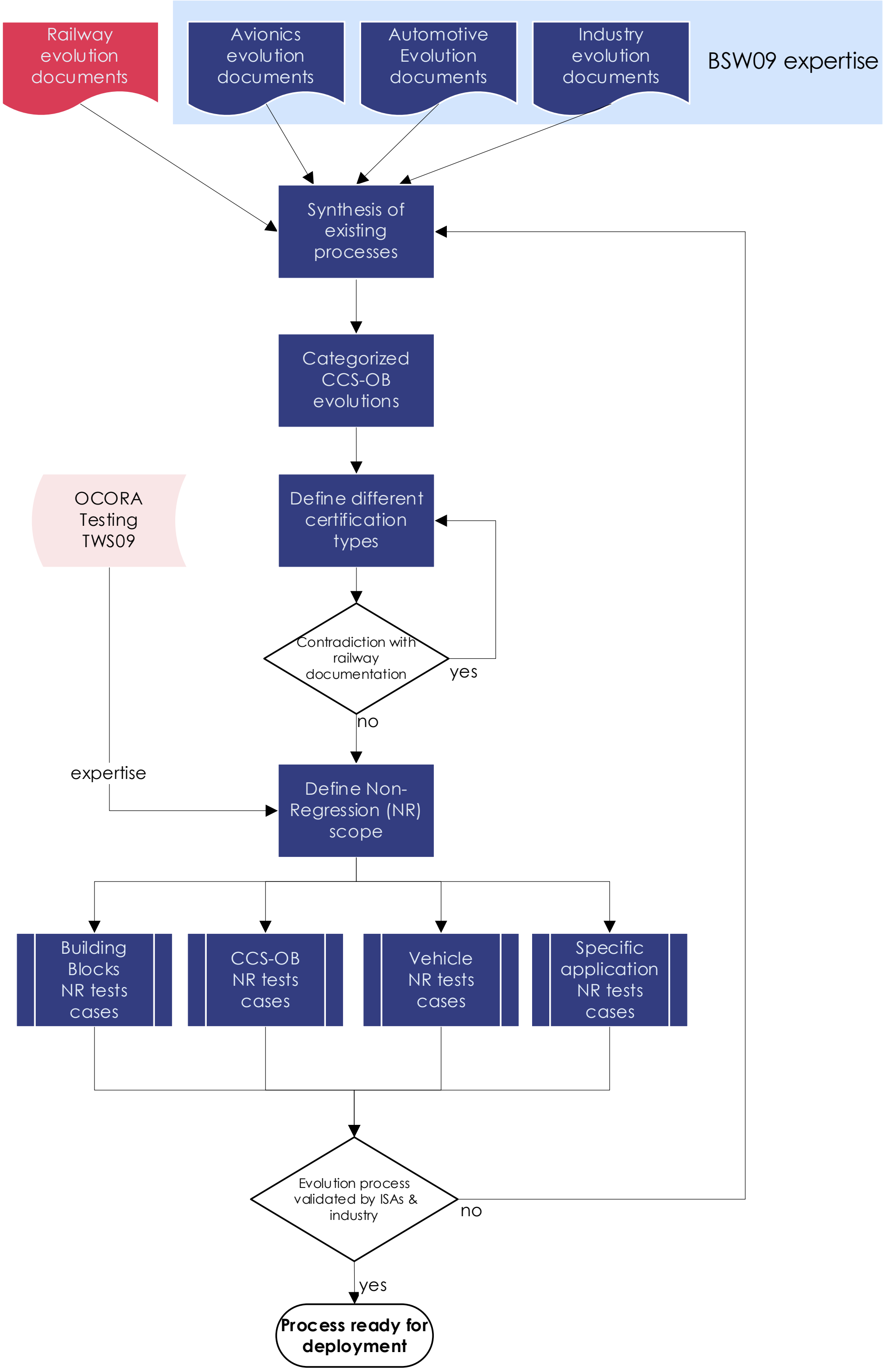

Railway evolution documents
Avionics evolution documents
Automotive Evolution documents
Industry evolution documents
BSW09 expertise
Synthesis of existing processes
Categorized CCS-OB evolutions
OCORA Testing TWS09
Define different certification types
Contradiction with railway documentation
yes
no
expertise
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:

- *Synthesis of existing processes*: research of existing railway documentation applicable when dealing with evolutions:
    - Railway documentation under consideration is identified in §2.3,
    - 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 R3, no useful documentation regarding evolution was found,
    - 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 R3, no useful documentation regarding evolution was found.,
  - Electronical Industry sector (e.g. https://www.fairphone.com/en/). This should be analyzed in future OCORA releases; it is not considered up to OCORA R3.

Unfortunately, some research was made in the light rail sector (e.g. metro, tramway, …) and no standardized process dealing with evolution was found. Such processes exist only at suppliers' level and are therefore not accessible and not standardized.

The activity of analyzing other sectors standards is the task of the BWS09 – Acceptance of Global Standards group. Up to R3, 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:

- The redundancy between the different processes (if any),
- The strengths of each process,
- The weaknesses of each process,
- Its adaptability to the railway world.

- *Categorized CCS-OB evolutions*: 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 12.
- *Define different certification types*: one key activity of this process is to propose different shades of assessments based on the evolution impact. This is presented in §2.7.
- *Define Non-Regression (NR) tests scope*: for the last step, the Testing group of OCORA (i.e. TWS09) will join the RAMS team (i.e. TWS07) to define a typical scope of non-regression tests for each type of classified evolutions:
    - For each building block or type of building blocks (L2) (this will be clarified in a future release of OCORA),
    - For the CCS OB (L3) integrating the evolved building block(s),
    - For the vehicle hosting the CCS OB (L4) through the Train Adapter defined by OCORA,
    - For the specific application represented (L5) by the vehicle in its dedicated network. The vehicle authorization, as required by Directive 2018/545 [24] is done at this final step.

  The different integration levels (i.e. L1 to L5) are defined in the OCORA Testing Strategy [13].

  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 detail in section 5. 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 does not lead to a contradiction or incompatibilities with existing railway standard or directive.

If the previous condition is reached, the process will be shared 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 [11] which is a complementary document to be applied after the evolution management process (refer to [11]).

In today's standard related to the interoperability world, directive CSM-RA [23] 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 [24].

CCS OB is basically covered by its scope in CSM-RA [23]:

> *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 [22]:
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 [23]: *(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 [23]:*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 [23], CENELEC standard EN 17023 [20] has also been analysed during this whitepaper realisation. Indeed, the latter uses the same criteria, with the same definition, as defined in CSM-RA [23] 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 [23] and EN 17023 [20] 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 [23] where the modifications management are presented inEN 50129 [18]:

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 [22]
  - 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 [11]).

These "evolutions" refer 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 .

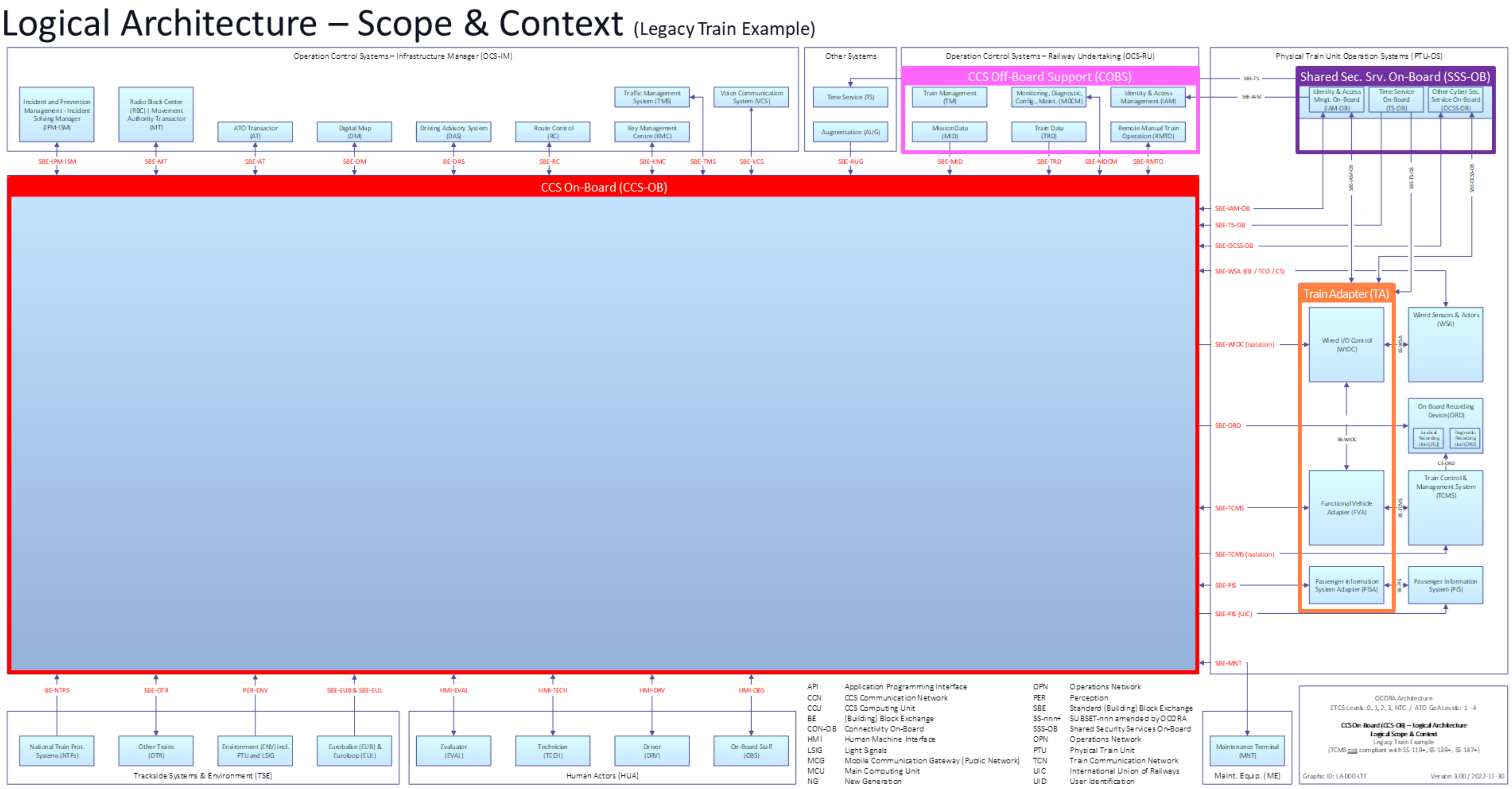
Evolutions are a central key element of OCORA to reach the seven design goals defined in Guiding Principles [6]:

- ***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, Train Adapter, and the SSSB (cybersecurity) in purple as described in the System Architecture document [8]. They are represented by the red and orange frames on Figure 5. The CCS OFF-board Support (COBS) it our of the sxcope for this process (pink frame).

It must be noticed that the Train Adapter will, on a longer run, not be useful anymore and therefore be 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 [11].


Logical Architecture – Scope & Context (Legacy Train Example)
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)
Digital Map (DM)
Driving Advisory System (DAS)
Route Control (RC)
Traffic Management System (TMS)
Key Management Centre (KMC)
Voice Communication System (VCS)
SBE-IPM-ISM
SBE-MT
SBE-AT
SBE-DM
BE-DAS
SBE-RC
SBE-KMC
SBE-TMS
SBE-VCS
Other Systems
Time Service (TS)
Augmentation (AUG)
SBE-AUG
Operation Control Systems – Railway Undertaking (OCS-RU)
CCS Off-Board Support (COBS)
Train Management (TM)
Monitoring, Diagnostic, Config., Maint. (MDCM)
Identity & Access Management (IAM)
Mission Data (MID)
Train Data (TRD)
Remote Manual Train Operation (RMTO)
SBE-MID
SBE-TRD
SBE-MDCM
SBE-RMTO
Physical Train Unit Operation Systems (PTU-OS)
SBE-TS
SBE-IAM
Shared Sec. Srv. On-Board (SSS-OB)
Identity & Access Mngt. On-Board (IAM-OB)
Time Service On-Board (TS-OB)
Other Cyber Sec. Service On-Board (OCSS-OB)
SBE-IAM-OB
SBE-TS-OB
SBE-OCSS-OB
CCS On-Board (CCS-OB)
SBE-IAM-OB
SBE-TS-OB
SBE-OCSS-OB
SBE-WSA (EB / TCO / CS)
Train Adapter (TA)
Wired I/O Control (WIOC)
Wired Sensors & Actors (WSA)
BE-WSA
SBE-WIOC (isolation)
On-Board Recording Device (ORD)
Juridical Recording Unit (JRU)
Diagnostic Recording Unit (DRU)
SBE-ORD
BE-WIOC
CE-ORD
Functional Vehicle Adapter (FVA)
Train Control & Management System (TCMS)
BE-TCMS
SBE-TCMS
SBE-TCMS (isolation)
Passenger Information System Adapter (PISA)
Passenger Information System (PIS)
BE-PIS
SBE-PIS
SBE-PIS (UIC)
SBE-MNT
BE-NTPS
SBE-OTR
PER-ENV
SBE-EUB & SBE-EUL
HMI-EVAL
HMI-TECH
HMI-DRV
HMI-OBS
National Train Prot. Systems (NTPs)
Other Trains (OTR)
Environment (ENV) incl. PTU and LSIG
Eurobalise (EUB) & Euroloop (EUL)
Trackside Systems & Environment (TSE)
Evaluator (EVAL)
Technician (TECH)
Driver (DRV)
On-Board Staff (OBS)
Human Actors (HUA)
Maintenance Terminal (MNT)
Maint. Equip. (ME)

API	Application Programming Interface	OPN	Operations Network
CCN	CCS Communication Network	PER	Perception
CCU	CCS Computing Unit	SBE	Standard (Building) Block Exchange
BE	(Building) Block Exchange	SS-nnn+	SUBSET-nnn amended by OCORA
CON-OB	Connectivity On-Board	SSS-OB	Shared Security Services On-Board
HMI	Human Machine Interface	OPN	Operations Network
LSIG	Light Signals	PTU	Physical Train Unit
MCG	Mobile Communication Gateway (Public Network)	TCN	Train Communication Network
MCU	Main Computing Unit	UIC	International Union of Railways
NG	New Generation	UID	User Identification

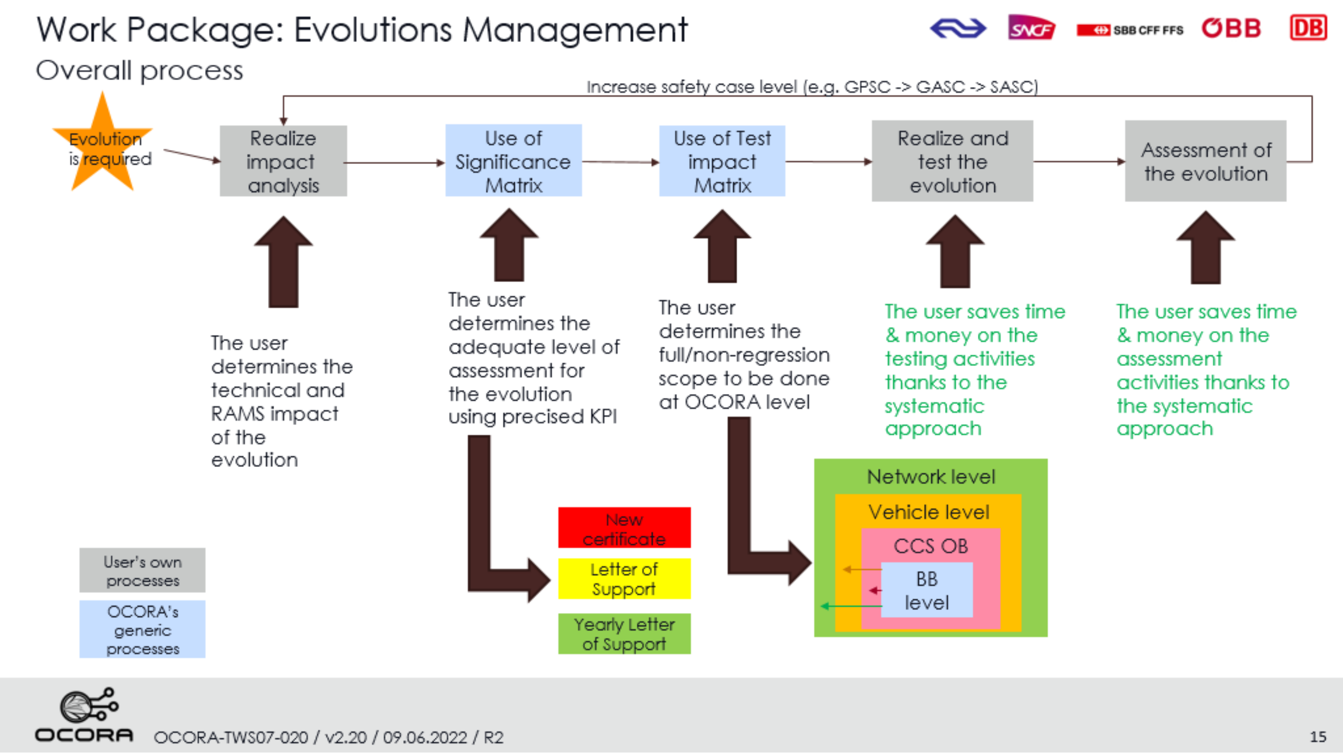
OCORA Architecture
ETCS-Levels: 0, 1, 2, 3, NTC / ATO GoA Levels: 1 - 4

CCS On-Board (CCS-OB) – Logical Architecture
Logical Scope & Context
Legacy Train Example
(TCMS not compliant with SS-119+, SS-139+, SS-147+)

Graphic ID: LA-000-LTE
Version 3.00 / 2022-11-30

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 between 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 [13] and introduced in section 5.
- 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 [11] 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:

- Building Block (BB) Suppliers: 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 minor 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, fix of a cybersecurity issue). The way to quantify "small" evolutions is described in the "Significance Matrix" in Table 1.
- Builder/Integrators (i.e. at CCS OB, vehicle and system levels as defined in the Testing Strategy [13]): 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 [22] 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 on the repartition of the roles by the contracting entity who is responsible for the whole contract of new vehicles or retrofit projects.

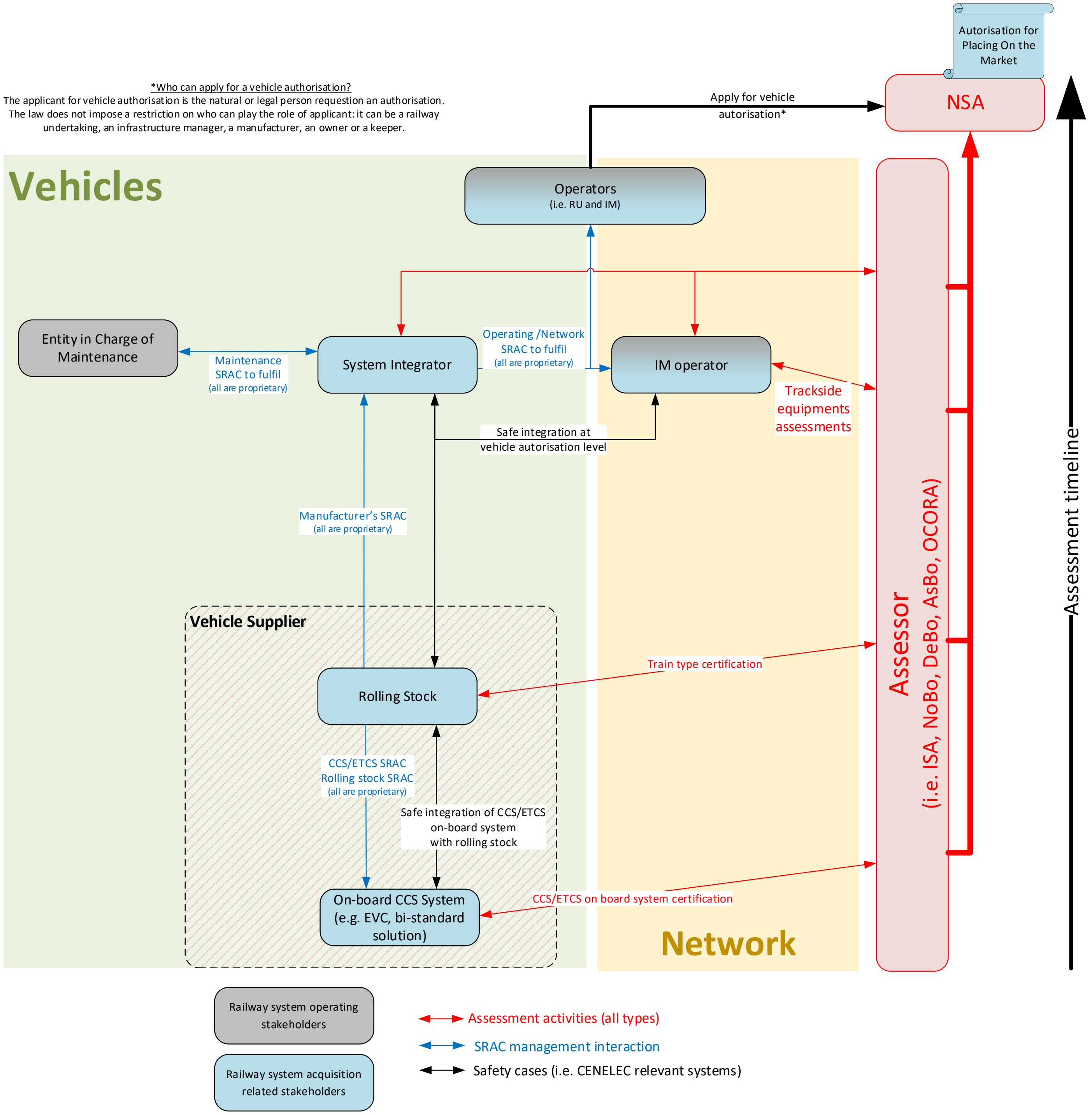

*Who can apply for a vehicle authorisation?
The applicant for vehicle authorisation is the natural or legal person requestion an authorisation.
The law does not impose a restriction on who can play the role of applicant: it can be a railway undertaking, an infrastructure manager, a manufacturer, an owner or a keeper.
Autorisation for Placing On the Market
NSA
Apply for vehicle autorisation*
Vehicles
Operators
(i.e. RU and IM)
Entity in Charge of Maintenance
Maintenance SRAC to fulfil
(all are proprietary)
System Integrator
Operating /Network SRAC to fulfil
(all are proprietary)
IM operator
Trackside equipments assessments
Safe integration at vehicle autorisation level
Manufacturer's SRAC
(all are proprietary)
Vehicle Supplier
Rolling Stock
Train type certification
CCS/ETCS SRAC Rolling stock SRAC
(all 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
Network
Assessor
(i.e. ISA, NoBo, DeBo, AsBo, OCORA)
Assessment timeline
Railway system operating stakeholders
Railway system acquisition related stakeholders
Assessment activities (all types)
SRAC management interaction
Safety cases (i.e. CENELEC relevant systems)

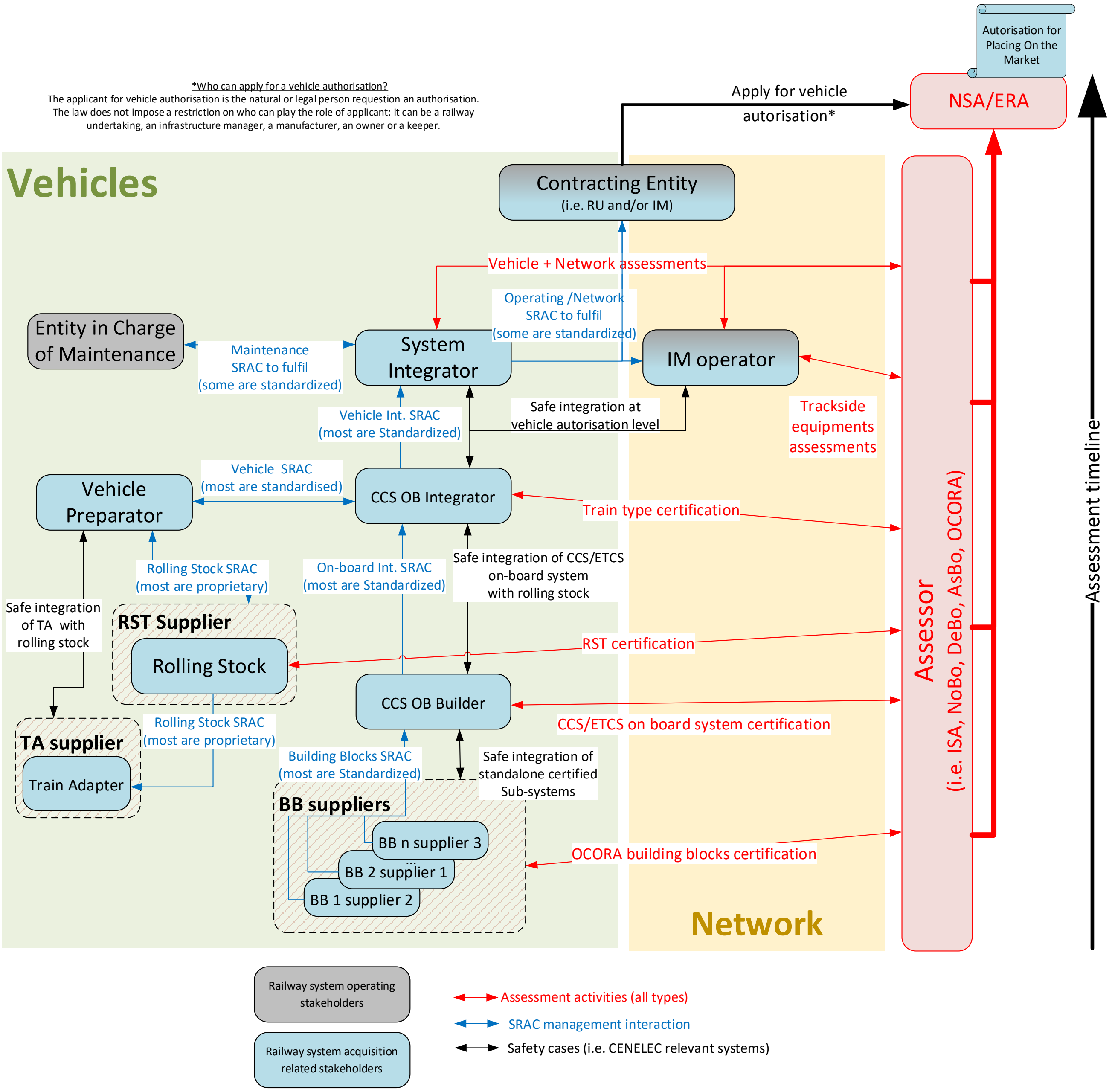
Figure 7 Classic of current ERTMS approval process

Figure 8 tends to present a possible future ERTMS approval that integrates OCORA requirements. **It must be understood that the assignment of the BB suppliers, CCS-OB Builder, vehicle preparator, CCS-OB integrator and system integrator are not defined by OCORA**. However, OCORA defines a frozen list of stakeholders for OCORA based projects including their responsibilities and interactions between each other's. This is defined in the Optimized Approval Process [11]. Each contracting entity is responsible for assigning these roles to chosen actors.

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.

Autorisation for Placing On the Market
NSA/ERA
Apply for vehicle autorisation*
Vehicles
Contracting Entity (i.e. RU and/or IM)
Vehicle + Network assessments
Operating /Network SRAC to fulfil (some are standardized)
Entity in Charge of Maintenance
Maintenance SRAC to fulfil (some are standardized)
System Integrator
IM operator
Vehicle Int. SRAC (most are Standardized)
Safe integration at vehicle autorisation level
Trackside equipments assessments
Vehicle Preparator
Vehicle SRAC (most are standardised)
CCS OB Integrator
Train type certification
Rolling Stock SRAC (most are proprietary)
On-board Int. SRAC (most are Standardized)
Safe integration of CCS/ETCS on-board system with rolling stock
Safe integration of TA with rolling stock
RST Supplier
Rolling Stock
RST certification
CCS OB Builder
CCS/ETCS on board system certification
TA supplier
Train Adapter
Rolling Stock SRAC (most are proprietary)
Building Blocks SRAC (most are Standardized)
Safe integration of standalone certified Sub-systems
BB suppliers
BB n supplier 3
BB 2 supplier 1
...
BB 1 supplier 2
OCORA building blocks certification
Network
Assessor
(i.e. ISA, NoBo, DeBo, AsBo, OCORA)
Assessment timeline
Railway system operating stakeholders
Railway system acquisition related stakeholders
Assessment activities (all types)
SRAC management interaction
Safety cases (i.e. CENELEC relevant systems)

Figure 8 Future ERTMS approval process including OCORA

The complete decomposition of the two above pictures is defined in the Optimized Approval Process. The main task is to define the activities handled by the three integration steps. Their scopes of activities have to be defined for:

- First realization of an OCORA compliant CCS OB (i.e. retrofit of an existing vehicle or new vehicle). This will be supported by the Optimized Approval Process,
- Evolution of the OCORA compliant CCS OB once certified. This will be supported by the current process and the Optimized Approval Process.

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

The latter, detailed in Directive 2018/545 [24], 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 [25] 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 complete assessment is mandatory and when it can be replaced by a lighter set of assessment activities without degrading the overall safety level of the SuC.

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

EN 50129 [18] 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, the former EN 50506-2 [21] provided 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 a struggle when deploying this modifications process 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 and parameters 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 does not implement clear separation between safe and non-safe parts.

In the current process, the naming “segregated BB” is used anytime a reference is made to a building block designed according to the separation rules defined by OCORA which are recapped hereafter (the complete list may be updated in a future release of OCORA:

- strict separation between safe (i.e. SIL1 to SIL4) and non-safe (i.e. basic integrity or not safety related) elements,
- strict separation between elements developed according to different SIL (e.g. SIL2 and SIL4),
- strict separation between cybersecure (i.e. SL 1 to SL 4) and non-cybersecure (i.e. SL 0) elements,
- strict separation between elements developed according to different SL (e.g. SL 2 and SL 4),
- strict separation between safe (i.e. SIL1 to SIL4) and cybersecure (i.e. SL 1 to SL 4) elements.

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 shows that already today, some industry suppliers have defined granular assessments in their proprietary modular systems.

Three 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 concerns non-safety related SuC.
- **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 (or when integrated above evolved BB) occurs.

  The activities consist for the supplier or the CCS OB Builder to follow his internal quality management process to handle the modification, save it in its records, increase the version (i.e. a standardized versioning management will be proposed in a future release of OCORA) of the SuC 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 thanks to an addendum to the last valid certificate. The quantification of “minor” is the purpose of the significance matrix defined in section 3. The letter of support represents a delta 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 [18] 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 evolutions for major evolutions (refer to section 3)

3 Significance evaluation process and matrix for assessment

3.1 Significance process

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.

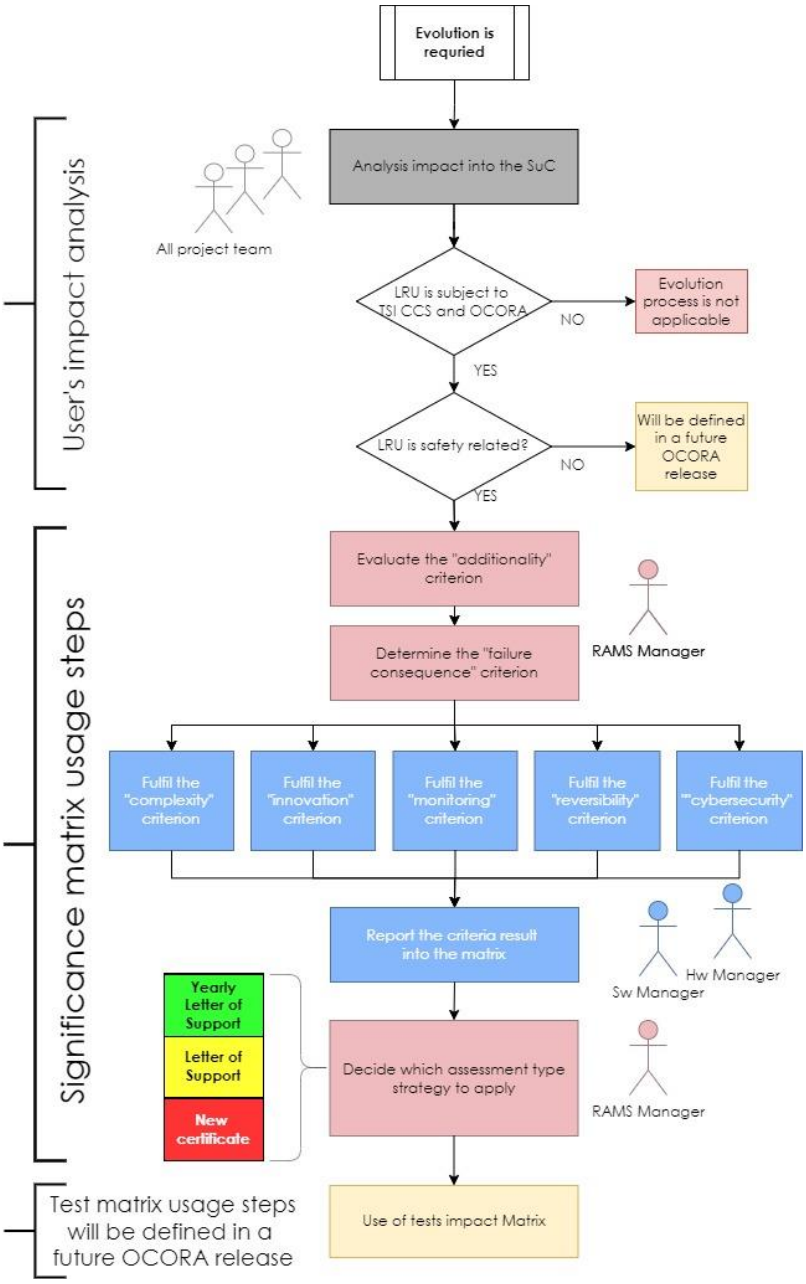

Evolution is requried
User's impact analysis
All project team
Analysis impact into the SuC
LRU is subject to TSI CCS and OCORA
NO
Evolution process is not applicable
YES
LRU is safety related?
NO
Will be defined in a future OCORA release
YES
Significance matrix usage steps
Evaluate the "additionality" criterion
RAMS Manager
Determine the "failure consequence" criterion
Fulfil the "complexity" criterion
Fulfil the "innovation" criterion
Fulfil the "monitoring" criterion
Fulfil the "reversibility" criterion
Fulfil the ""cybersecurity" criterion
Report the criteria result into the matrix
Sw Manager
Hw Manager
Yearly Letter of Support
Letter of Support
New certificate
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 12 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 R3 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.

3.2 Significance Criteria

3.2.1 Additionality

The first criterion defined in CSM-RA [23] 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.

3.2.2 Failure consequence

The second criterion defined in CSM-RA [23] 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;*

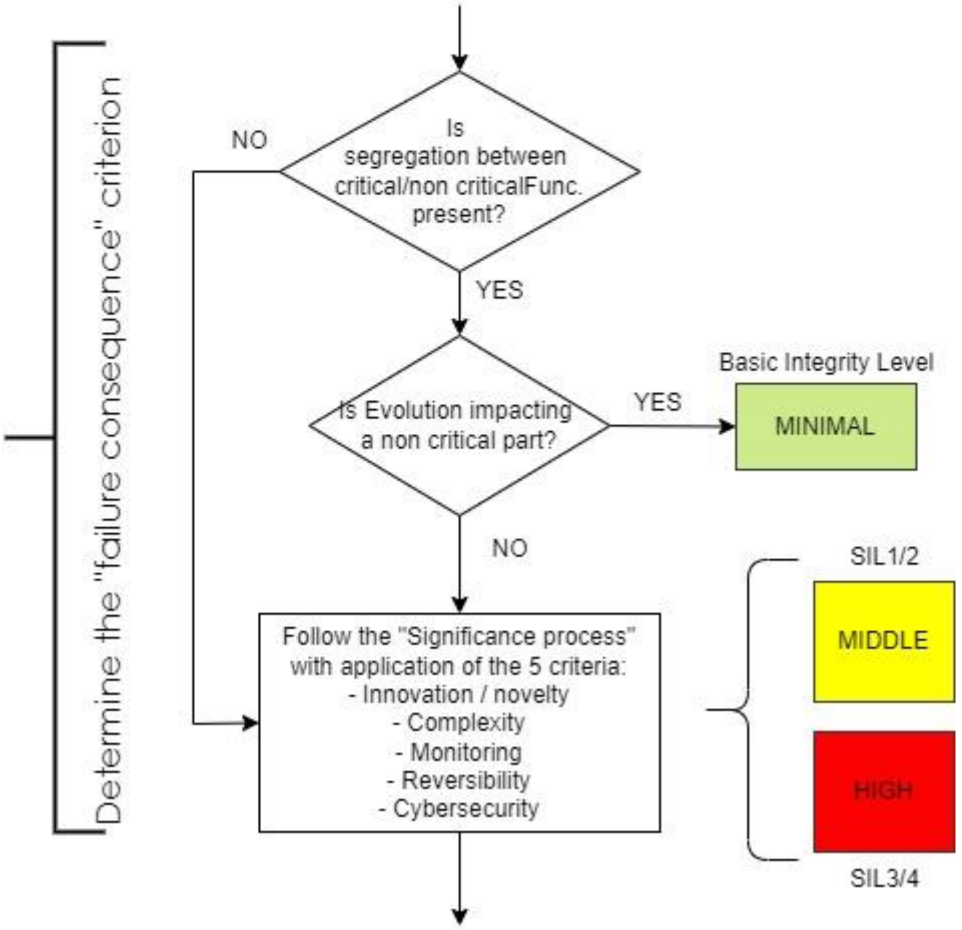

Determine the "failure consequence" criterion
Is segregation between critical/non criticalFunc. present?
NO
YES
Is Evolution impacting a non critical part?
YES
Basic Integrity Level
MINIMAL
NO
Follow the "Significance process" with application of the 5 criteria:
- Innovation / novelty
- Complexity
- Monitoring
- Reversibility
- Cybersecurity
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 criteria 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 Table 1, (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 criteria 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 CYBERSECURITY	HIGH MINIMAL	🟩	🟥	🟥
	MIDDLE LOW	🟩	🟥	🟥
	LOW MIDDLE	🟩	🟨	🟥
	MINIMAL HIGH	🟩	🟨	🟨
FAILURE CONSEQUENCE :		MINIMAL FAILURE CONSEQUENCE	MIDDLE FAILURE CONSEQUENCE	HIGH FAILURE CONSEQUENCE
		NoSIL BIL/SIL0	SIL 1/2	SIL3/4

SIGNIFICANCE :

SIGNIFICANCE IMPACT		ASSESSMENT METHOD
🟩	MINIMAL IMPACT	Yearly Letter of Support
🟨	MIDDLE IMPACT	Letter of Support
🟥	MAXIMUM IMPACT	New Certificate

Table 1 Significance matrix

The following criteria aim at choosing the line in the matrix (see Table 1) from “MINIMAL” to “HIGH”.

3.2.3 Innovation/novelty

The third criterion defined in CSM-RA [23] 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 [26], 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 Table 1):

- 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”,

3.2.4 Complexity

The fourth criterion defined in CSM-RA [23] 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,
  - Application of a Software Complexity Metrics standard,
- 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).

3.2.5 Monitoring

The fifth criterion defined in CSM-RA [23] 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”.

3.2.6 Reversibility

The sixth criterion defined in CSM-RA [23] 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 Table 1) 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 [20] provides two other examples of combinations:

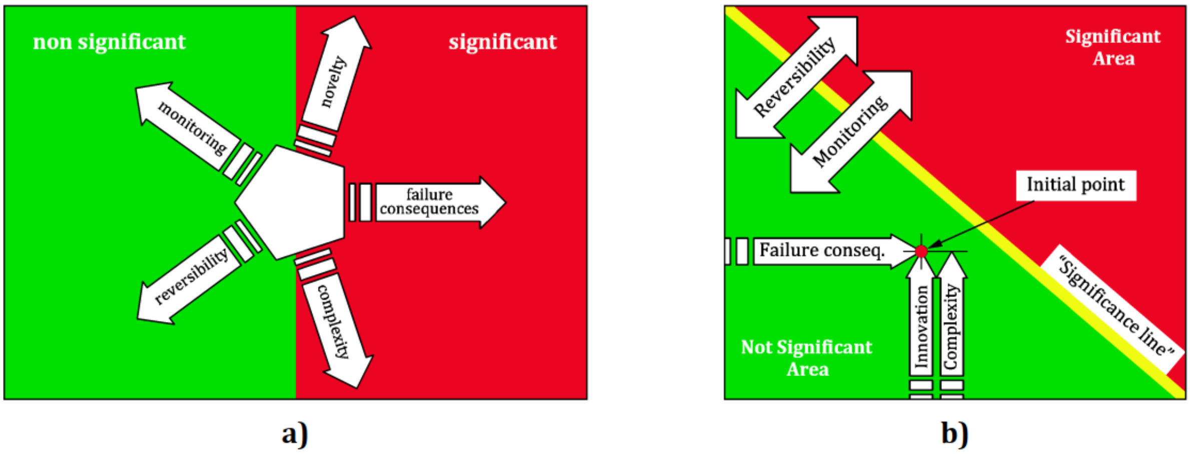


Figure 11 Diagram of Safety Significance Analysis from EN 17023 [20]

In OCORA context, the matrix presented on Table 1 is proposed because it seems easier to deploy than other examples from EN 17023 [20]. 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 four 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 builder 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. OCORA has defined in section 8 a list of such metrics to help each user at defining its own (or reuse the ones from COORA).

3.2.7 Cybersecurity

In the future it is likely that cybersecurity attacks on safety-related systems on-board of rolling stock will be more common than now for several reasons:

- more connectivity of the systems,
- use of open and common communication protocols,
- hybrid warfare by enemy countries,
- ransomwares,
- …

To face these future challenges, it is necessary to define a process that will allow the fast deployment of new software versions / security patches aimed at reducing the risk of a cyberattack by :

- correcting cybersecurity issues
- or implementing new cybersecurity measures.

To do so, in R3, “Cybersecurity Impact” is added to the previous EN 17023 [19] criteria.

To determine the MINIMAL to HIGH impact, the following cybersecurity criterion based on the §6.3.1 of the TS50701:2021 are used :

- Operational availability
- Financial Impact

		MINIMAL	LOW	MIDDLE	HIGH
CYBERSECURITY IMPACT	**Operational availability**	Important operation disturbed less than 1 day.	Most of operation disturbed between 1 h and 1 day Important operation disturbed between 1 day and 1 week	Most of operation disturbed between 1 day and 1 week. Important operation disturbed during more than 1 week	Most of operations disturbed during more than 1 week
	Financial impact	Impact not visible on annual basis	Impact in a significant way the organization annual benefits.	Impact in a significant way the organization annual budget (>10 % of revenue)	Could lead to organization bankrupt

Table 2 Cybersecurity impact

The higher the cybersecurity impact, the easiest the deployment of the evolution should be in order to correct the issue as fast as possible.

So as Monitoring and Reversibility, a HIGH Cybersecurity impact will lower the “Safety Score” of the Matrix:

	MINIMAL	LOW	MIDDLE	HIGH
INNOVATION	1	2	3	4
COMPLEXITY	1	2	3	4
MONITORING	4	3	2	1
REVERSIBILITY	4	3	2	1
CYBERSECURITY IMPACT	4	3	2	1

Table 3 Management of cybersecurity impact weight

3.2.8 Example of Use of the matrix

Let’s consider an OS security patch on a software SIL2 correcting a security issue that could have a high financial impact:

We analyse each criterion and affect it from MINIMAL to HIGH.

	MINIMAL	LOW	MIDDLE	HIGH
INNOVATION	1	2	3	4
COMPLEXITY	1	2	3	4
MONITORING	4	3	2	1
REVERSIBILITY	4	3	2	1
CYBERSECURITY IMPACT	4	3	2	1

Table 4 Example of attribution of criteria’s weight

The impact value of each criterion is then added to each other and divided by the number of criteria (5).

In our example, the Safety Score equals to: (1 + 1 + 1 + 1 + 1) / 5 = 1

The score is reported in the matrix:

As the System is SIL2 and the Score 1 is inferior to 2, the modification is categorized as MINIMAL (green colour in the
Table 1).

↓

= 4	HIGH	🟩	🟥	🟥
3 < x < 4	MIDDLE	🟩	🟥	🟥
2 < x < 3	LOW	🟩	🟨	🟥
<= 2	MINIMAL	🟩	🟨 X	🟨
		BIL	SIL1 / 2	SIL3 / 4

Table 5 Example of matrix usage

As the Safety Impact is MINIMAL, a Letter of Support is sufficient.

4 Software development process

Although they are mainly dedicated to new developments, the EN50128:2011 (applicable for software for railway control and protection systems) and EN50657:2017 (applicable for any other software on board rolling stock contributing to operational functions) are highly recommended to be used for software evolutions. Therefore, they are widely used by the industry for such purposes.

Note: Other industries' standards (avionics, automotive, …) could also be used for software evolutions. BB suppliers could prefer to use such standards, but this possibility will not be developed for R3 as it not common nowadays.

Two types of evolutions are listed in the EN50128:2011 and EN50657:2017 standards:

- minor
- major

In case of a major evolution, these European standards should be applied in their entirety.

For a minor evolution only one chapter of the standards should apply: §9.2 "Software Maintenance", which allows to use a much lighter process of development.

Minor evolutions can be developed much faster than majors (less documentation and tests for example). Therefore, they can be deployed much faster on the CCS, which will be very convenient for evolutions such as security patches, maintenance events, etc...

It is up to the supplier to decide whether an evolution is minor or major.

The decision then should be submitted to the software's assessor's evaluation:

- for any modification for software developed according to the EN50128:2011
- for SIL1-4 software developed according to the EN50657:2017.

As these standards do not define what is a minor and a major evolution and it can be difficult to define it.

This why OCORA proposes to use the following process.

After having determined if a modification has a LOW, MIDDLE or HIGH significance impact according to Table 1, the supplier shall use the following table:

Significance of the software modification according to Table 1	**Complexity**	**Type of software modification according to §9.2 of the EN50128:2011 and EN50657:2017**	**Software modification process to apply**
MINIMUM IMPACT	-	minor	Application of §9.2 of the EN50128:2011 / EN50657:2017
MIDDLE IMPACT	MINIMAL or LOW	minor	Application of §9.2 of the EN50128:2011 / EN50657:2017
	MIDDLE or HIGH	**major**	Application of the full process of the EN50128:2011 / EN50657:2017
MAXIMUM IMPACT	-	**major**	Application of the full process of the EN50128:2011 / EN50657:2017

Table 6 Corresponding table between Significance Impact and Software modification process

5 Hardware development process

Unfortunately, the software maintenance process defined in EN 50128 and EN 50657 has no equivalent into EN 50129 for hardware maintenance. The maintenance of hardware elements during the lifetime of the SuC is nevertheless a reality which is faced by all suppliers. This concerns for instance obsolescence management, performance optimization such as FFF (Fit, Form and Function) replacement of some components (most of time discrete) by new references that present better functional performance, better immunity to EMC disturbances…

This process aims at defining rules for hardware evolutions that can be considered as minor and will therefore lead to request a yearly letter of support or letter of support instead of a new certificate. The final criteria list will be provided in a future release of OCORA. However, a first batch of them are available in section 8.

6 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 [13] and is further developed in the present section.

It must be noticed that up to R3, 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 12 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 12 presents the focus of testing activities, depending on the SuC under evolution.

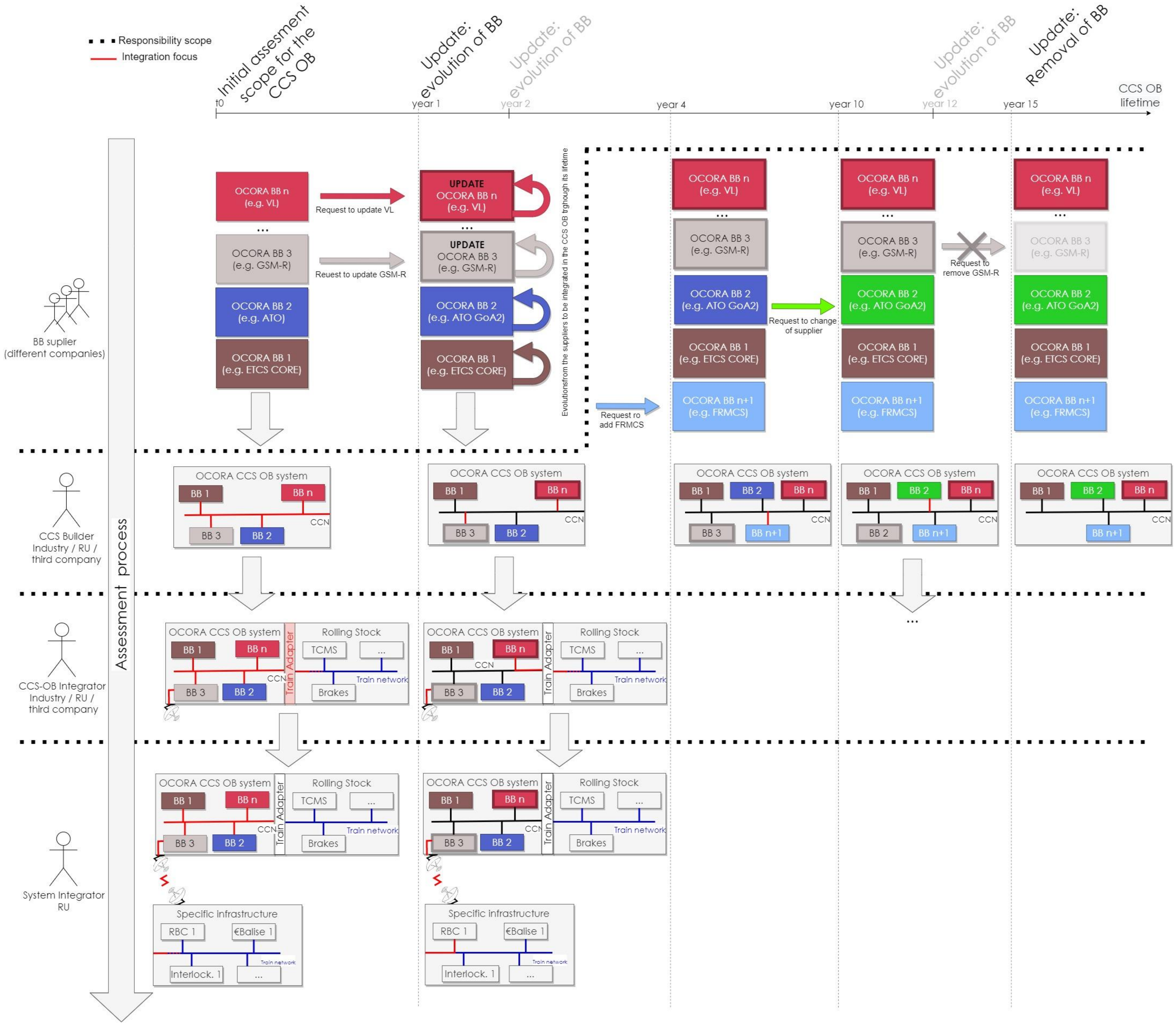


Figure 12 Overall evolution process representation

6.1 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 [13].

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 builder 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 [13]). This kind of tests focus on the integration of the building blocks used as “black-box” by the CCS OB builder.

The CCS OB builder (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 CCS OB 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 [13]) is applicable.

The CCS OB 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 [11]. The strategy on the reuse of the first vehicle type on additional fleet is covered by the Optimized Approval Process [11].

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 [13]) 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 [11]. This ends with the first Authorization for Placing on the Market document as required by [24] and developed in the Optimized Approval Process [11].

In order to avoid at maximum, the potential extra costs of implementation of an OCORA modular CCS OB for the first time (e.g. management of the two new roles of CCS OB builder and CCS OB integrator), a complete guideline is scheduled to be provided as good practices for any stakeholder involved. This will be delivered in a future release of OCORA.

6.2 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 12 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 builder 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 builder 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 (i.e. black box) 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 CCS-OB 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 [11] (see Figure 6) for the management of the European authorizations defined by [24].

6.3 Addition of a new building block in the CCS OB system

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 6.1.

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 CCS-OB 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.

6.4 Removal of a building block in the CCS OB system

This kind of evolution will occur when a CCS OB builder 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 R3):

- 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.

7 Update and configuration management

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

OCORA supports investigations to allow safe and secure “over the air” updates of the building blocks, likely when train will be in the depot after the train journey. The process to manage that will be defined in a future release of OCORA. This will be realized in coordination with the TWS08 – MDCM and the TWS06 – Cybersecurity team in R4. Indeed, this process, despite being suitable from an operational point of view must be compliant with the expectations of:

- RAM and most of all maintainability,
- Safety for SIL1 to SIL4 building blocks,
- Cybersecurity for SL 1 to SL 4 elements.

The first common paper dealing with an update process for OCORA compliant systems is proposed in [12]. The latter has been reviewed by RAMSS members of OCORA.

8 Annex – Proposition of metrics for CSM-RA criteria

The present annex aims at providing some hints for the process implementers to quantify each criterion defined by the CSM-RA:

- FAILURE CONSEQUENCE,
- ADDITONALITY,
- INNOVATION,
- COMPLEXITY,
- MONITORING,
- REVERSIBILITY,
- CYBERSECURITY IMPACT

“Cybersecurity impact” is a new criterion introduced by OCORA in R3 and so far, not taken in account by CSM-RA. However, for the future OCORA compliant building blocks and CCS-OB, evolutions related to cyber-security are likely to be more frequent than the ones dealing with safety issues and functionalities upgrades.

So far, the proposed list hereafter is just a set of proposed metrics that may be revised and refined in future release of OCORA. So far, they are presented here as informative.

FAILURE CONSEQUENCE and ADDITIONALITY are completely defined

		MINIMAL	LOW	MIDDLE	HIGH
INNOVATION	a) no technical code of practice (e.g. norms) can be used for the modification because it does not exist yet	**YES / NO**	**YES / NO**	**YES / NO**	**YES / NO**
	b) the modification has not been successfully deployed (i.e. no critical failure of the modification has been detected so far) on similar products/system in commercial revenue	**YES / NO**	**YES / NO**	**YES / NO**	**YES / NO**
	c) the modification goes beyond the actual state of technique (e.g. FRMCS, ATO GoA 3/4) Note: no competitors have similar products already on the market	**YES / NO**	**YES / NO**	**YES / NO**	**YES / NO**
	d) The modification does not correspond to the reference system defined by TSI CCS 2016 (and when applicable 2022)	**YES / NO**	**YES / NO**	**YES / NO**	**YES / NO**
COMPLEXITY	**Hardware**	To be defined in a future release of OCORA	Replacement / addition of other component(s) (e.g. resistors, capacitors) where all failures modes are clearly identified in Annex C of EN 50129	Modification / new of a PCB (i.e. defined in adequacy to EN 50124)	Replacement / addition of a UPIC (e.g. obsolescence management, improvement of performances). Note: this refers to the components covered by Annex F of EN 50129

		MINIMAL	LOW	MIDDLE	HIGH
	Software	Bug fixing/improvement (i.e. no modification of SRS) - MINIMAL amount of source code/modules/tests impacted ("MINIMAL" is to be quantified by each user) - Difficult comprehensibility of the evolution: NO	Bug fixing/improvement (i.e. no modification of SRS) - LOW amount of source code/modules/tests impacted ("LOW" is to be quantified by each user) - Difficult comprehensibility of the evolution: NO	Bug fixing/improvement (i.e. no modification of SRS) - MIDDLE amount of source code/modules/tests impacted ("MIDDLE" is to be quantified by each user) - Difficult comprehensibility of the evolution: YES	- Impact on a system function(s) / service (i.e. change of SRS) - HIGH amount of source code/modules/tests impacted ("HIGH" is to be quantified by each user) - Difficult comprehensibility of the evolution: YES
		Use of metrics rules (i.e. D.37 from EN 50657) From MINIMAL to HIGH rules	Use of metrics rules (i.e. D.37 from EN 50657) From MINIMAL to HIGH rules	Use of metrics rules (i.e. D.37 from EN 50657) From MINIMAL to HIGH rules	Use of metrics rules (i.e. D.37 from EN 50657) From MINIMAL to HIGH rules
	Safety	No change of Sw/Hw	To be defined in a future release of OCORA	Modification / addition of SRAC(s)	- Modification of a safety mechanism (e.g. Hw or Sw watchdog, built in test) without safety issue - Modification of one or several safety analysis document (e.g. FMEA, FTA, MARKOV) - Management of a safety issue (i.e. safety related change request without mitigation)
	Technical file (i.e. documentation used for the assessment) **Note: testing are not considered as DESIGN documents**	Important level of modified QUALITY/MANAGEMENT documents from previous assessment (e.g. < 10% of the QUALITY/MANAGEMENT technical file documents used for the assessment)	- Important level of modified USER documents from previous assessment (e.g. < 10% of the RAILWAY OPERATION technical file documents used for the assessment) - Important level of modified QUALITY/MANAGEMENT documents from previous assessment (e.g. > 10% of the QUALITY/MANAGEMENT technical file documents used for the assessment)	- Weak level of modified DESIGN documents from previous assessment (e.g. < 10% of the DESIGN technical file documents used for the assessment) - Important level of modified RAILWAY OPERATION documents from previous assessment (e.g. > 10% of the RAILWAY OPERATION technical file documents used for the assessment)	Important level of modified DESIGN documents from previous assessment (e.g. > 10% of the DESIGN technical documents used for the assessment)
	Mechanical	Modification of mounting parts (e.g. screws, rail)	Impact on the weight (i.e. increase and then not be in conformity with RU's target)	Modification of connectors, rack, cabinet	N/A
	Electrical	Modification of simple components (e.g. fans, lights, horns)	Modification of a complex equipments (e.g. EMC filter)	Modification of a complex equipments (e.g. power supply)	N/A

		MINIMAL	LOW	MIDDLE	HIGH
	Manufacturing	Change of other machine or method (e.g. placing of component, varnish)	Change of test equipment or method (e.g. routine, serial, burn-in)	N/A	N/A
	Organization				
	Installation, commissioning, and maintenance	To be defined in a future release of OCORA	- Adapt maintenance/driver/Network (i.e. infrastructure) documents - Workshops/Trainings (e.g. new skills required)/Work instruction for the workers needed - Update of existing Sw/Tool	-New Software/Tool needed (e.g. new service Sw, new laptop, new Hw tool) - More resources due to the higher complexity (e.g. more time required) - Creating new processes (e.g. new testing/validation process) - Modification of the facilities (e.g. train depot, new tests equipments)	N/A
MONITORING		No detection at all. The modification is not monitored	Defect is detected by the maintenance people after it occurs during depot checks (e.g. periodic maintenance checks) There is no code nor information point that a failure has occurred	Defect is detected by the maintenance people after it occurs during depot checks (e.g. periodic maintenance checks) There is a information point that a failure has occurred	Defect is detected before it happens. The modification is covered by a built-in test that directly warns the driver/maintenance people
REVERSIBILITY		A retrofit is possible but need the complete replacement of the LRU (e.g. Hw spare parts not available, to be redesigned)	A retrofit is possible but need the complete replacement of the LRU (e.g. available Hw spare parts)	A retrofit is possible but need to be physically connected to the LRU without send it back to the manufacturer (e.g. local Sw/Hw downgrade)	A remote (i.e. Over The Air) retrofit is possible with possible synchronous multiple modifications (i.e. Sw updates/downgrades only) => such as Tesla
CYBERSECURITY IMPACT	*Operational availability*	Important operation disturbed less than 1 day.	Most of operation disturbed between 1 h and 1 day Important operation disturbed between 1 day and 1 week	Most of operation disturbed between 1 day and 1 week. Important operation disturbed during more than 1 week	Most of operations disturbed during more than 1 week
	Financial impact	Impact not visible on annual basis	Impact in a significant way the organization annual benefits.	Impact in a significant way the organization annual budget (>10 % of revenue)	Could lead to organization bankrupt