EU-RAIL SYSTEM PILLAR

PRAMS Plan - Evolution management of safety-related modular systems - Process and organisation

PRAMS Plan - Evolution management of safety-related modular systems - Process and organisation

Author(s)	SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) , Kertis, Tomáš (SMO RS EN EH CZ PRO ASR) , JAGEL Marc , Iñigo Iruretagoyena Tormo , Markus Spindler (Rail Expert Consult) , Julien Bois
Abstract	Document presenting a safety guideline for handling evolutions in a modular architecture
Config Item	PRAMS Plan
Document ID	Evolution Mngt Process/PRAMS_Plan_-_Evolution_Management_in_a_Modular_Architecture#830161 PRAMS Plan - Evolution management of safety-related modular systems - Process and organisation
Classification	Public
Status	In Progress (first discussion in domain started)
Version	1.2
Revision	830161
Last Change Date	19.02.2026
Copyright	Brussels: Europe's Rail Joint Undertaking, 2026

This work is currently a work in progress. The content presented is subject to change as it undergoes further review, refinement, and development. Please do not consider this version as final or authoritative.

INFO: History table is not displayed, because this document is in status **doc_inprogress**.
RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }
CONTACT: For more information contact Administrator

Approval for reviewers

Type of Approval	Document Review

Approval for approvers

Approvals	CIUCCI Paolo : Approved
Type of Approval	Document Approval

Table of contents

Table of Figures

Table of Tables

1 Preamble

Polarion Work Items
This document is written using Polarion.
Several work items are used to contain the text and diagrams :

- Text
- System Requirement
- Rationale
- Issue
- Definition

Each Work Item is identified by a unique auto-generated ID SPPRAMSS-xxxx and has a title written in Bold. **[**SPPRAMSS-14697, Text **]**

Open Points
Open Points are marked as Polarion Work Items "Issue" in this document.
Their text is highlighted in orange. **[**SPPRAMSS-14694, Text **]**

1.1 Purpose

Content of the document
The present document covers the following aspects:

- Analysis of the current standards and directives regarding evolutions management (refer to SPPRAMSS-5667 - State of the art),
- Proposition of a new generic approach to determine the significance of evolutions in modular systems (refer to SPPRAMSS-1167 - Significance process),
- Proposition of a development process following evolutions (refer to SPPRAMSS-5674 - Software development process and SPPRAMSS-5678 - Hardware development process)
- Proposition of a new generic approach to determine the minimum required testing activities (refer to SPPRAMSS-5679 - Testing Process)
- Proposition of different shades for homologation depending on the evolution(s) impact (refer to SPPRAMSS-5683 - Assessment Process)

[SPPRAMSS-985, Text **]**

Purpose
The purpose of the current process is defined into the PRAMS User Stories and reflects the Pain Point List . **[**SPPRAMSS-8878, Text **]**

Introduction to the evolution management
Any upgrade and update of railway subsystems as described in SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] within their operational phase is burdened by SPPRAMSS-9973 - Homologation and safety processes, which are in practice rigorous, rendering operational evolution challenging and costly.

Evolution management addresses the need for railway operators and suppliers to oversee improvements to railway systems in operation, considering the complexity of homologation processes. It aims to maintain or enhance safety standards while minimizing service interruptions.

The foundation of evolution management within the SP PRAMS group traces back to the OCORA project. Its significance to the PRAMS group is evident, as it guarantees the safe, secure, and seamless improvement of the railway system. **[**SPPRAMSS-7343, Text **]**

Motivation to the evolution management

The railway industry, operators, and other rail undertakings face significant challenges in adapting to the dynamic nature of the real world, while adhering to conservative safety processes. The introduction of evolution management is motivated by several factors:

1. The ***significant change assessment*** of the CSM-RA can vary greatly across different system levels, including infrastructure construction, rolling stock, and cyber-physical systems within rail automation. There may be variations in approach among railway entities.
   Evolution management aims to provide guidelines on managing changes across these different levels and approaching re-certification and safety assessment processes.
2. Any updates to systems within operations are subject to evaluation regarding the significance of change, as mentioned in paragraph above. It is not always clear whether functions that are seemingly unrelated to safety may impact safety and to what extent. Operators also face challenges in managing hazard logs resulting from technical aspects introduced by suppliers. Operators seek to streamline the ***process of implementing any changes, updates, security patches, or renewals*** during the operational phase of railway products, ***with minimal impact on homologation processes*** (considering that 90% of SP scope is CCS).
3. On the other hand, there is pressure on suppliers from the railway sector (operation and maintenance) and safety standards regarding modularity. Modularity comes in various forms, and determining the appropriate level of granularity is crucial. Achieving modularity goals can be done through different means, some of which involve computing platforms using SPPRAMSS-7490 - Multiple Independent Levels of Security or Safety. Technologies deployed to achieve modularity at logical and software levels offer numerous advantages, but also pose challenges from a safety perspective. This document aims to outline the ***pros and cons of fundamental modularization technologies*** from a safety point of view to meet the objectives of evolution management.
4. Additionally, the PRAMS Plan within the System Pillar has proposed ideas for the design-based safety case. The ***Design Based Safety Case is a mean to achieve the simplification of the safety and homologation process***, reflecting the principles of evolution management described within this document while aiming to maintain or even improve overall safety.

[SPPRAMSS-7344, Text **]**

Links with other working groups

This document is connected with the work being carried on by other Europe's Rail working groups:

- System Pillar - Train CS, Traffic CS, Computing Environment, Cyber-security, Transversal
- Innovation Pillar - FP2 R2DATO WP26 "Modular Platform Specification"

[SPPRAMSS-14395, Text **]**

1.2 Scope

Limitation of scope for the first and second version

This document is a deliverable from the PRAMS team in SP. This team intends to deliver guidelines and methodologies that are applicable to all domains of SP. However, the first two releases of this document are limited to the CCS systems (i.e. covered by SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] and developed in Task 2 CCS domain) which cover most of the SP domains.

In a next version, the scope of the document will be extended to any railways system.
For example :

- DAC (see System Concept_Central Instance - Part A WP4_3)
- Trackside assets
- Axle counters
- FRMCS

[SPPRAMSS-1001, Issue, Open, SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) **]**

Document part of the STIP
This document has been presented in the STIP¨under the ID STIP_86. This documents will, once validated by all reviewers, an enabler for regulation updates (e.g. CENELEC standards, CSM) to allow a better evolution management for modular architectures. **[**SPPRAMSS-15811, Text **]**

Vehicle authorisation process and trackside approval
This document focuses on CCS systems only. The simplification of vehicle authorisation and trackside approvals is outside the scope of this document. However, it represents the next step of safety optimisation for modular architecture and therefore, this topic shall be further developed by the PRAMS team
Finally, the two processes PRAMS Plan - Evolution management of safety-related modular systems - Process and organisation and Specification for Authorisation, Integration and Upgradeability of modular train CS system including train interface shall be strongly connected and shall be deployed by any future project to exploit the full potential of the modular architecture. **[**SPPRAMSS-1036, Issue, Open, Bois Julien (I-NAT-GST-CCS-EXT - Extern) **]**

Benefits of evolutions in a modular architecture
The need of deploying a modular architecture in the CCS systems is presented in Common Business Objectives. In accordance with the Common Business Objectives, this document tends to provide benefits for all the stakeholders using modular systems thanks to smooth evolutions:

- Building Block (BB) suppliers: the standardisation of different certification levels requiring different shades of documentation to be updated aims at avoiding a systematic new certificate request to the assessor. This will greatly ease the management of minor evolutions (e.g. change of non-critical item inside a safe part, fix of a cybersecurity issue). The way to quantify “minor” evolutions is described in SPPRAMSS-1167 - Significance process;
- Builder/Integrators (i.e. at CCS, vehicle and system levels as defined in SPPRAMSS-1099 - "Safe integration" in a modular architecture): the evolution management process defines standardised 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 integration of the evolved building blocks or CCS systems.
- Assessors: the official release of the document will be sent for review to several ISA and NoBo from the NB Rail organisation. The benefit for them is that this process provides clear frames for the different homologation 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 homologation scope;
- Railway Undertakings / Infrastructure managers: the process allows to accelerate the update of the deployed vehicles or networks equipped with modular systems and reduce drastically costs. The “big steps” as presented in SPPRAMSS-1026 - CCS OB example of slow evolutions will be replaced by more frequent “small steps” composed of minor evolutions with strong benefits in time and costs development for the projects.

It must be noticed that all the benefits presented above must not degrade the overall PRAMS level of the different projects. It may, at the opposite, reinforce it. The objective behind is that; from a lifetime perspective, it is considered safer to handle:

- **a breakdown into a number of CCS sub-systems (i.e. building blocks) having a smaller technical scope and more frequent updates following a systematic approach compared to**
- **the current monolithic CCS systems having wider technical scope and less frequent updates based on proprietary approach to deal with them.**

The architecture team made the following statement in SPT2ARC-1252 : [SPPRAMSS-1091, Text **]**

Benefits for competition in the market: Smaller sub-systems allow more suppliers...
Benefits for **competition in the market**: Smaller sub-systems allow more suppliers to compete. The problem per sub-system is smaller and can be solved (i.e. a product can be provided) even if a particular supplier is not able to develop the entire CCS system. Also, the subdivision of the entire system into

smaller components/sub-systems require a better specification, so that implementing should be easier. This is increasing competition in the market. Benefits for testability: With smaller harmonised subsystems there is the opportunity to capitalize (and solve) on the return of experience on failures having common occurrence. **[**SPT2ARC-1252, Analysis **]**

1.3 Intended audience

Evolution Management process intended audience
This document is intended for the following users:

- PRAMS engineers outside ERJU dealing with building block realisationand/or integration,
- Safety assessors outside ERJU,
- Any other stakeholder from the railway sector.

Comments will be handled by the PRAMS team but they cannot block the delivery of the document in case of disagreement with the PRAMS team. **[**SPPRAMSS-15810, Text **]**

1.4 Document Context

Input from OCORA
The present document uses as input the process defined by OCORA in SPPRAMSS-9974 - [OCORA release R3]. **[**SPPRAMSS-1003, Text **]**

1.5 Glossary

1.5.1 Terms and definitions

No references

- Adaptability
Adaptability refers to the ability to adjust a system in response to changes in its environment or changes of requirements. It involves a broader concept of flexibility and resilience, encompassing not only modifications to the system itself but also its capacity to accommodate evolving needs or external factors. An adaptable system can respond effectively to new technologies, market demands, user expectations, or regulatory changes. **[**SPT2ARC-940, Definition **]**

- Application Condition
Application conditions are specific conditions imposed on external entities that interact with the system under consideration. They are also precise requirements about the environment and use of the system under consideration in its application. The following list contains examples for application conditions:

- skills of maintenance people that need to be trained
- operators of the system
- requirements about the physical environment
- maintenance processes ("exported constraint, relevant for users").
- physical needs
- temperatures of server rooms
- engineering rules
- precautions in installation and testing
- rules and methods for maintenance and fault-finding
- safety-related ones (SRAC) and RAM-related ones (RAM RAC)

Note: Application Conditions shall not be used to export requirements to another system or subsystem. If something is expected from another level 3 system or subsystem, it shall first go through ARC domain who will derive it. This ensures clear entry points for subsystems, improve completeness of analysis by considering the big picture when more than one sub-system is involved.

Addtional note: External should be more specific in the frame of System Pillar. This could be external to system level 2 (so external to CCS and TMS etc.). This to avoid having subsystems (system level 3 and higher) exporting requirements to each other instead of having them clearly defined at global system with appropriate system analysis. In the context of System Pillar, "external" has to be understood as "external to CCS system" for tasks/domains, system level or analysis phase (OA, SA, LA or PA).
[SPPR-3728, Definition **]**

- Changeability
Changeability refers to the ease with which a system can be modified or customized to meet specific requirements or adapt to new circumstances. It encompasses both minor changes, such as configuration adjustments, and more substantial modifications, such as adding or removing sub-systems. **[**SPT2ARC-939, Definition **]**

- conformity assessment body
a body that has been notified or designated to be responsible for conformity assessment activities, including calibration, testing, certification and inspection; a conformity assessment body is classified as a ‘notified body’ following notification by a Member State; a conformity assessment body is classified as a ‘designated body’ following designation by a Member State **[**SPLI-219, EU Directive 2016/797 (v200528), Definition **]**

- Error correction
Error corrections are a type of evolutions, covered by the Evolution management process. Several types of error correction at building block level can occur:

- error correction of the TSI, because it is incorrect (curently not covered by the Evolution Management process).
- error correction of the specification, because it is not compliant with the TSI.
- error correction of the specification, because it is incorrect
- error correction of the source code, because it is not implementing correctly the specification i.e. "deviating from intended functions and/or performance".

Error corrections are basically defined in:

- SPPRAMSS-4525 - [Directive 2016/797] (Article 16) and
- SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] (section 6.5 Management of errors and 7.2.10)

More details are defined in SPPRAMSS-14396 - Error correction.
[SPPRAMSS-15261, Definition **]**

- Evolvability
Evolvability is the ability to easily adapt to new technologies or to extend the functionality of the CCS system without the involvement of the original supplier. **[**SPT2ARC-808, Definition **]**

- Homologation
In the railway context, *homologation* refers to the formal approval process that ensures a railway system, component, or piece of equipment meets all relevant safety, technical, and regulatory standards before it can be put into operation. This process involves rigorous testing, certification, and validation by authorized bodies (e.g. ERA) to confirm that the railway elements, such as trains, signaling systems, and infrastructure, comply with national and international standards.

The process typically includes a series of assessments, including safety, interoperability, performance, and environmental impact evaluations, before final approval is granted for commercial use.

This term is used as a "generic" term that covers any aspect related to certification, assessment, authorisation, approval, acceptance. **[**SPPRAMSS-9973, Definition **]**

- Patch
A patch is a small software update that fixes bugs, security vulnerabilities, or minor issues.
It corresponds to the PATCH version in Semantic Versioning (SEMVER), indicating backward-compatible without adding new features (e.g. SPPRAMSS-15261 - Error correction, system improvements, unexpected system behavior). **[**SPPRAMSS-14487, Definition **]**

- SECURITY
The protection resulting from all measures, also administrative ones, to prevent accidental or malicious modification or disclosure of data; for key management, the protection generally guarantees confidentiality, authenticity and integrity of keys. **[**SPLI-1031, Subset-023 (v4.0.0), Definition **]**

- Scalability
Scalability refers to the ability of a system/sub-system to handle an increasing workload or expand its capacity without significantly impacting performance, efficiency, or cost. **[**SPT2ARC-1011, Definition **]**

- Sub-system (sometimes called “Building Block”)
Sub-systems are along ARCADIA systems on System Level 5. Not to be confused with sub-systems in the TSI / interoperability directive. In the TSI / interoperability directive context a sub-system shall be regarded as a interoperability constituent
A sub-system is a part of a system, which is not split into smaller entities. It represents a leaf element in the hierarchy of systems-of-systems.
Physically speaking, a sub-system is either a piece of hardware plus software, or just a piece of software.
A sub-system is a source able unit of the CCS system, in particular:

- a sub-system can be individually tendered to a supplier,
- a sub-system can be built individually by a supplier,
- a sub-system must be integrated into a system, which includes all necessary test, verification, certification and validation activities depending on the level of harmonisation.

The harmonisation of the sub-system’s features is to be defined according to the requested level:

- Functional Apportionment,
- Interoperability,
- Exchangeability, or
- Interchangeability.

[SPT2ARC-1013, Definition **]**

- Testability
A sub-system that is designed for testability will be ready to show that it fulfils the requirements needed by the overall system. Testability is not an attribute of the sub-system/module itself but has to be designed into architecture and interfaces. **[**SPT2ARC-1286, Definition **]**

- Updateability
Updateability refers to the ability of a system to receive and incorporate updates or patches, e.g. to address security vulnerabilities. Updates are often provided to improve the performance of the system, stability, or security without introducing significant changes to its functionality. **[**SPT2ARC-937, Definition **]**

- Upgradeability
Upgradeability refers to the ability of a system to undergo significant enhancements or improvements in terms of its features, functionality, or performance. Upgrades typically involve the installation of a newer version or release of the system that offers new capabilities or improved performance compared to the previous version. **[**SPT2ARC-936, Definition **]**

- Virtual Building Block
A virtual building block is a virtualised SPT2TS-1828 - Building Block, also referred by other working groups as a SPT2CE-694 - Functional System . **[**SPPRAMSS-15977, Definition **]**

1.5.2 Introduction to terminology dealing with evolution

Basic orientation on the use of 'evolution' in ERJU
The transformation of the railway system(s) in Europe is described by the ERJU documentation along four central terms:

- evolution
- migration
- change
- adaptation

and the respective abilities to perform these: evolvability, scalability, changeability and adaptability.
So what is the difference, and why bother using different terms? After all, basically, you can call every alteration to a system (or a system of systems or components thereof) a change.
So here in short why, how and what is done in this respect throughout ERJU documentation:

Evolution 1.5.2.1-1 is used whenever the perspective goes beyond a specific alteration of a specific object (be it a component, (sub) system or the railway system) to a broader view, be it by including the environment of the altered system in the considerations or be it by considering a series of alterations intended to take place along a timeline. So evolution is much related to a '**system view**'. The use of 'evolution' is **restricted to** cases where the system under consideration is the **System Pillar Reference Architecture** or a subsystem thereof. Where systems not complying to or not part of the System Pillar Reference Architecture are considered, a different term must be used - this is how migration comes into play:
The same '**system view**' as for evolution is applied when the term **migration 1.5.2.2-1** is used - but in this case, the considerations cover cases where the **system initially does not comply to the harmonised architecture** while the alterations are intended to transform the system (now or after additional steps) to comply with the harmonised architecture.

Change 1.5.2.3-1 is the term used whenever considering a **particular** alteration of a given object. **If** that change is **necessitated by the environment** of the given object, the term **adaptation 1.5.2.4-1** is used. This helps to differentiate it from the case where a change is made as a deliberate decision (and the idea or request for the change might be rejected or neglected). As adaptations are kind of forced on the object under consideration, from the object's point of view the ability to perform these changes is in some sense more interesting than the adaptations themselves, that's why the term **adaptability** is way more frequently used than the term adaptation.
More detail is given in the following work items focusing on one term each: **[**SPPRAMSS-9925, Text **]**

1.5.2.1 Evolution term

How the term Evolution is used in ERJU
Evolution is used from a system perspective (see SPT1RS-84 - The System view) and is used in particular for changes in the target railway system (defined by ERJU) along its innovation path:
SPT2MIG-1779 - Evolution
Evolution is the process of gradually developing, refining or improving parts of the System Pillar Harmonized Operational Processes respectively the System Pillar's reference architecture.
Evolution is mentioned in one of the seven goals of the EU Rail Master Plan SPT1RS-150 - EURAIL Goals :
Harmonised approach to evolution and greater adaptability
Evolution is covered by or related to Common Business Objectives along the topics of
SPT1RS-113 - Optimize safety strategies and standards

- SPT1RS-232 - simplified standard safety components
- SPT1RS-231 - validated system performance, robust PRAMSS framework

- SPT1RS-230 - safety logic with generic safety approval
- SPT1RS-229 - seamless and selective exchange of components under production
- SPT1RS-228 - vehicle is interoperable without local integration test

SPT1RS-116 - Reduce the system complexity by optimal design to ease regulatory compliance

- SPT1RS-238 - simplify certificates and their impacts

Evolution is expected to be managed centrally, at least when concerning interfaces:
SPT1RS-114 - Reinforced role for rail in European transport and mobility
[...] Systems interfaces should be highly standardized and promote interoperability within the SERA. The evolution of this should be centrally managed to ensure coherence and consistency of system performance.[...] **[**SPPRAMSS-9923, Text **]**

Evolution in the context of the CENELEC standards
Evolutions in the context of this document refer to the activities realised in the whole lifecycle of SPPRAMSS-349 - [EN 50126-1:2017] for railways systems with higher focus on the Phase 11: Operation, maintenance and performance monitoring and section 9.2 - Software maintenance of SPPRAMSS-8814 - [EN 50716:2023] for railways software developments.

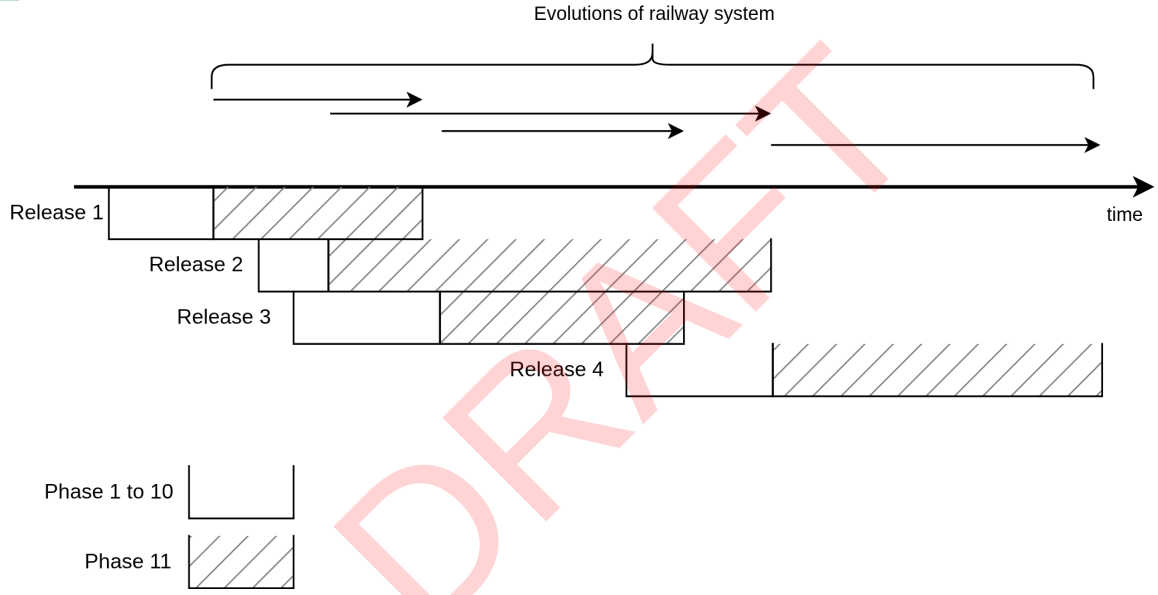


Figure 1 Lifecycle of railway systems

[SPPRAMSS-14401, Text **]**

The relevance of Evolution and its management to PRAMS
The definition of evolution, as described above, refers to the gradual development and refinement of a system over time, through a process of adaption and improvement within the System Pillar's reference architecture. Evolution is often driven by the need to improve system reliability, efficiency, or other key metrics, while addressing new or changing needs and challenges. It can be assumed that a CCS building

block or system/ subsystem have already been certified according to:

- NoBo independent conformity assessment defined in SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]
- Interoperability certificate (i.e. design examination certificate)
- ISA certificate (i.e. compliance to CENELEC standards)
- DeBo examination report (only when dealing with NNTR) or
- System pillar requirements (refer to Specification for Authorisation, Integration and Upgradeability of modular train CS system including train interface and SPPRAMSS-9981 - TrafficCS homologation aspects)

The changes needed to achieve the desired evolution of the system refer to a delta of one or several elements contained in the technical file of the SPPRAMSS-8882 - System under Consideration which is presented in the safety case between the last certified version and the current one. This way, the individual changes, often referred as SPPRAMSS-14903 - Change Request, might affect a large number of documents and cause a huge amount of work if changeability and evolution of the respective components/interoperability constituents/subsystems/systems and their PRAMS documentation is not managed properly; in particular, if the easy integration into the system embedding the SuC (and the authorisation of that embedding system) is not provided for.
A basic insight driving ERJU is: Evolution of the System Pillar Harmonized Operational Processes and the System Pillar Reference Architecture will only be possible based on an effective and highly performant configuration management, a modular architecture and authorisation processes reflecting the modular architecture.
This is why Evolution Management in a Modular Architecture is a key topic from a PRAMS perspective. **[**SPPRAMSS-1075, Text **]**

Technical Files and Patches
A Change Request to the CCS shall be written in the next contract to ensure that patches are excluded from the Technical File (Z number of the X.Y.Z SEMVER versioning). **[**SPPRAMSS-15262, Issue, Open **]**

TrafficCS homologation aspects
Up to SC2.3, only TrainCS dealt with authorisation aspects and reviewed by the PRAMS team.
The scope shall be enlarged to also cover the trackside homologation aspects with TrafficCS and PRAMS domains.
See SPPRAMSS-11455 - To Do List to solve the Traffic CS issue **[**SPPRAMSS-9981, Issue, Open, Morman Bettina (I-NAT-GST-CCS) **]**

1.5.2.2 Migration term

How the term Migration is used in ERJU
Migration is used from a system perspective (see SPT1RS-84 - The System view) and is used in particular for the process of converting existing CCS/TMS systems and processes to the harmonized System Pillar Reference Architecture:
SPT2MIG-1776 - Migration
Migration is the national or company specific process of converting existing CCS/TMS systems including operational processes to corresponding systems and processes of the harmonized System Pillar's reference architecture.
with
{c} SPT2OD-6743 - [Stakeholder] Configuration management designed to facilitate economic migration paths
as a key constraint to achieve not only migration goals, but ERJU goals in general.
Migration and deployment is listed in Europe's Rail's multi annual work programme (https://rail-research.europa.eu/wp-content/uploads/2022/03/EURAIL_MAWP_final.pdf) as one of the key drivers for the System Pillar to improve the European railway system:

The System Pillar shall also define, assess and deliver possible migration paths between the various current railway control & command architectures existing among Europe and a harmonized future European railway control & command architecture, building upon input at national level.
Migration is mentioned in the context of the core objectives of Europe's Rail:
SPT1RS-80 - The ambitious objectives for Europe’s Rail
[...] ensuring the system is maintained, error-corrected and able to adapt over time and ensure migration considerations from current architectures [...]
The System Pillar must cover migration plans that would bridge research and innovation, industrialisation and deployment of innovative technologies, operational concepts and overall solutions. The System Pillar will endeavor to simplify and reduce the costs for the different stages in deployment for the target system including authorisation procedures to ensure safety and security.
Migration is covered by or related to Common Business Objectives along the topic of
SPT1RS-117 - Fast migration and Rollout

- SPT1RS-237 - efficient migration based on adaptable systems
- SPT1RS-234 - viable migration path
- SPT1RS-235 - viable forward/backward compatibility

Due to its overall importance, migration is addressed by its own System Pillar domain, SPT2-Migration, which is defining the concepts and principles for migration to be applied (see SPT2MIG-411 - DP2.3 CCS and TMS Migration Principles), including SPT2MIG-1778 - Migration Plateau **[**SPPRAMSS-9924, Text **]**

1.5.2.3 Change term

How the term Change is used in ERJU
Change is used from a 'object-under-consideration' perspective for all systems, subsystems, components, building blocks etc. as the most general term to describe a difference between before and after, as described by SPT2MIG-534 referring to **changeability** (SPT2ARC-939 - Changeability):
“Changeability” shall be the overarching term for all other known terms in this context, like upgradeability, updateability, exchangeability, integrability, etc.
Most of the related terms are defined in a section of SPT2ARC-545 - System Concept_CCS - Granularity Concepts and Principles - Main
In an important additional view on things, SPT2ARC-1592 - Figure #: Levels of Harmonisation highlights the relations between change and (the effort needed for) integration & authorisation on basis of different terms in the context of change.
SPT2-Migration has elaborated on change and changeability in the CCS/TMS context and defined a list of what can be considered a change (e.g.: change of hardware, additional software on hardware). See SPT2MIG-536 for the entire list.
Change and changeability are identified to be a main factor in reducing cost of the European rail system: *For deployment and change within railway systems, cost is a constraint to adaptation and faster deployment. [...] Affordable system updates are an enabler for rapid system modernisation, ensuring continuous increase of rail performance. IT deployments that amortise over a 40-year period (e.g. the lifespan of a train) are not an option.* (see SPT1RS-97 - Reduced costs)
Change and changeability therefore are covered by or related to Common Business Objectives along the topic of reduced costs:

- SPT1RS-194 - independent lifecycle, simple exchange
- SPT1RS-193 - automate lifecycle processes
- SPT1RS-192 - reusable right first time work - including *reusable safety cases*
- SPT1RS-191 - changeability : Processes are oriented along an ever-changing system.

and the related topic SPT1RS-99 - Deliver affordable system updates :

- SPT1RS-190 - Changeability and upgradeability(1)
  Changeability and upgradeability shall ensure business continuity along the life-cycle with optimised investment scheme.
- SPT1RS-189 - Changeability and upgradeability(2)
  The system design shall anticipate the need for updates at minimum effort [...]
- SPT1RS-188 - Changeability and upgradeability(3), simpilified integration
  [...] the capability to manage system integration of components, with clear objective of reasonable system updates of SW and digitalized system, is a crucial objective.

Moreover, change and changeability are covered by or related to Common Business Objectives along the topics of SPT1RS-111 - Standardize architecture and SPT1RS-117 - Fast migration and Rollout :

- SPT1RS-218 - modularity
- SPT1RS-233 - simple repeatable DevOps
- SPT1RS-235 - viable forward/backward compatibility

[SPPRAMSS-9921, Text **]**

1.5.2.4 Adaptability term

How the term Adaptation is used in ERJU
Adaptation, usually referred to in terms of **adaptability**, is used from a 'object-under-consideration' perspective for all systems, subsystems, components, building blocks etc., in terms of their ability to adjust in response to changes in their environment or changes of requirements, see SPT2ARC-940 - Adaptability. (Adaptability therefore is a special aspect of changeability.)
Side note: special attention should be given to the term SPP-2325 - Adapted product which describes a product compliant to only some System Pillar specifications, but not all. The idea behind this is to make current national products future ready (later connection or upgrade to SP compliant systems).
SPT2MIG-523 lists several methods to design an “adaptable” system. The CCS and TMS Migration Principles presented by SPT2-Migration gives a critical review on including adaptability in standardisation strategies SPT2MIG-319 and states:
Obviously, every adaption leads to higher and specific dependencies and bespoke solutions. This is the downside, and the migration support by the standard gets lost. The advantage is of course, that adaptability can be used to simplify legacy migration (connect legacy to standard systems), or to solve a local compliance problem (e.g. National Technical Rules or national regulations).
underlining the trade-off between short term and long term effects:
Adaptations reduce short-term cost and increase long-term cost and diversity. If too much adaptability is made possible then a standard can completely lose its reason of existence.
and concludes:
*In general **adaptability shall be avoided as much as possible and only be used in very urgent cases**. Otherwise, the business case of standardisation (“reusability”) gets lost very fast.*
Adaptability is mentioned in the context of the core objectives of Europe's Rail:
SPT1RS-80 - The ambitious objectives for Europe’s Rail
[...] ensuring the system is maintained, error-corrected and able to adapt over time and ensure migration considerations from current architectures [...]
Adaptability is mentioned in one of the seven goals of the EU Rail Master Plan SPT1RS-150 - EURAIL Goals :
Harmonised approach to evolution and greater adaptability
SPT1RS-109 - Harmonised approach to evolution and greater adaptability
[...] The time to fix an issue is also relevant when it comes to adaptations related to error correction or security patching. This is also relevant for continuously enhancing the system.[...]

Adaptability is covered by or related to Common Business Objectives along the topics of
SPT1RS-112 - Increase flexibility and adaptability of systems

- SPT1RS-226 - systems: extensible capacity, scalability(2)
  Adaptive design is a prerequisite for continuously fulfilling capacity and performance requirements besides being vital for sustained levels and quality of train services.
- SPT1RS-225 - flexible regulation supports development
  Regulatory framework that supports speedy technology development and implementation processes is a critical condition for adaptive design.

SPT1RS-117 - Fast migration and Rollout

- SPT1RS-237 - efficient migration based on adaptable systems
  Incremental deployments that increase complexity and costs, need to be replaced by an efficient and coordinated migration strategy, based on adaptable systems.

[SPPRAMSS-9922, Text **]**

1.5.3 Abbreviations

Acronym (abbreviation)	Full text (title)
PMAT	PRAMSS Management & Assurance Team

BB - Building Block
A BuildingBlock is a logical unit of the system that is bound to a sourceable physical equipment by means of a Basic Data Identifier having:

- standardised functionality or aggregates standard functionality it depends on
- may have standardised PRAMS requirements (including Tolerable Functional Failure Rate [TFFR]
- may have Safety Integrity Levels [SIL] for functions within the system border and Safety Related Application Conditions [SRAC])
- standardised cyber security requirements (including Security Level [SL] based on the security requirements, and Security Related Application Conditions [SRAC])
- may have (on lower levels) standardised interfaces (on all OSI Layers) towards other Building Blocks and/or external systems.

One equipment can host several BuildingBlocks (e.g in the case of a MultiObjectController) and may be separately sourceable from different suppliers and capable of being integrated by a third party (integrator).
A BuildingBlock is configured by one or more BuildingBlockConfigurations.

A BuildingBlock must have an unique identifier called **bbId (**that could be a technical system or subsystem identifier).
The bbIds are assigned by the integrator and are transferred to another physical unit in case of replacement.
Each bbId must be unique.
[SPT2TS-1828, Definition **]**

BIL - Basic Integrity Level
Integrity attribute for safety-related functions with a TFFR higher than (less demanding) 10−5.h−1 or for non-safety-related functions. **[**SPPRAMSS-11109, CENELEC, EN 50129:2018, “ Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling”, Definition **]**

CCS - Control-Command and Signalling
Control-Command and Signalling **[**SPPRAMSS-11099, Definition **]**

CCS OB - Control-Command and Signalling - Onboard
CCS OB refers to the SPLI-372 - On-board control-command and signalling part of the SPLI-83 - Control-Command and Signalling **[**SPPRAMSS-10184, Definition **]**

CCS TRK - Control-Command and Signalling - Trackside
CCS TRK refers to the SPLI-375 - Trackside control-command and signalling part of the SPLI-83 - Control-Command and Signalling. **[**SPPRAMSS-11100, Definition **]**

CR - Change Request
A formal request to modify existing software to correct an issue, add new functionality, or comply with updated standards or operational requirements. **[**SPPRAMSS-14903, Definition **]**

CSM-RA - Common safety method for Risk evaluation and Assessement
'common safety method for Risk evaluation and Assessement' means the methods describing the assessment of safety levels and achievement of safety targets and compliance with other safety requirements; SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] **[**SPPRAMSS-343, Definition **]**

DAC - Digital Automated Coupling
Digital Automated Coupling **[**SPLI-93, Definition **]**

DeBo - Designated Body
From DIRECTIVE (EU) 2016/797 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the interoperability of the rail system within the European Union:
(42) 'conformity assessment body' means a body that has been notified or designated to be responsible for conformity
assessment activities, including calibration, testing, certification and inspection; a conformity assessment body is
classified as a 'notified body' following notification by a Member State; a conformity assessment body is classified
as a 'designated body' following designation by a Member State; **[**SPPRAMSS-11101, Definition **]**

ERP - Enterprise Ressource Management
Enterprise Ressource Management **[**SPPRAMSS-11117, Definition **]**

FS - Functional System
A Functional System is a comprehensive set of self-contained Compartments, assumed to be provided as one product by a single vendor. Depending on its overall function, it has a specific SIL assigned.
[SPT2CE-694, Definition **]**

GASC - Generic Application Safety Case
Generic Application Safety Case (from SPPRAMSS-334 - [EN 50129:2018/AC:2019-04])
[SPPRAMSS-8881, Definition **]**

GPSC - Generic Product Safety Case
Generic Product Safety Case (from SPPRAMSS-334 - [EN 50129:2018/AC:2019-04])
[SPPRAMSS-8880, Definition **]**

IDPS - Intrusion Detection and Prevention System
An Intrusion Detection and Prevention System (IDPS) is a network security solution designed to monitor, detect, and prevent unauthorized access, misuse, or malicious activity on a computer network
[SPPRAMSS-11112, Definition **]**

ISA - Independent Safety Assessor
The role is defined in "Table G.4 — Role specification for Independent Safety Assessor" of SPPRAMSS-335 - [EN 50126-2:2017] **[**SPPRAMSS-11104, CENELEC EN 50126-2:2017, “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety, Definition **]**

LoS - Letter of Support
Letter of Support **[**SPPRAMSS-11116, Definition **]**

LRU - Line Replaceable Unit
Line Replaceable Unit **[**SPPRAMSS-11114, Definition **]**

SRU - Shop Replaceable Unit
Shop Replaceable Unit **[**SPPRAMSS-11113, Definition **]**

NB Rail - NB-Rail Association
The NB-Rail Association is an international non-profit organization of the Third-Party Conformity Assessment Body (Notified Body (NoBo), Designated Body (DeBo), Assessment Body (AsBo), Entity in Charge of Maintenance – Certification Body (ECM-CB)) in the European railway sector. The association is installed to support and to complement the activities of NB-Rail coordination group. **[**SPPRAMSS-11107, Definition **]**

NNTR - Notified national technical rules
Articles 13 and 14 of Interoperability Directive define the cases where national rules (NRs) can be notified and the procedure of notification of national rules by Member States.
The applicable national rules (NRs) for vehicle authorisation are recorded in IT tool RDD. In particular, rules for ETCS and GSM-R are listed in section 12 “On-board control command and signaling” in the parameters list defined in Commission Regulation (EU) 2015/2299.
The relevant NRs for fixed installation including Control Command and Signaling trackside subsystem have to be notified through SRD tool (i.e. https://www.era.europa.eu/domains/registers/srd_en)
[SPPRAMSS-11105, Definition **]**

NoBo - Notified Body
From DIRECTIVE (EU) 2016/797 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the interoperability of the rail system within the European Union:
(42) ‘conformity assessment body’ means a body that has been notified or designated to be responsible for conformity
assessment activities, including calibration, testing, certification and inspection; a conformity assessment body is
classified as a ‘notified body’ following notification by a Member State; a conformity assessment body is classified
as a ‘designated body’ following designation by a Member State; **[**SPPRAMSS-11102, Definition **]**

SC2.x - Specific Contract for Lot 2 of year x
This refers to the ERJU contracts for SP signed every year; SC2.1 for the first year of developmeent and so on. The SP domains are part of the "Lot 2" in the overall ERJU project (e.g. IP, SP).
[SPPRAMSS-11106, Definition **]**

SIL - Safety Integrity Level
Safety Integrity Level **[**SPLI-1065, Subset-023 (v4.0.0), Definition **]**

SuC - System under Consideration
System under Consideration (from SPPRAMSS-334 - [EN 50129:2018/AC:2019-04])
[SPPRAMSS-8882, Definition **]**

TMS - Traffic Management System
Traffic Management System **[**SPPRAMSS-15973, Definition **]**

TCMS - Train Control and Monitoring System
Train Control and Monitoring System **[**SPPRAMSS-11110, Definition **]**

yLoS - Yearly Letter of Support
Yearly Letter of Support **[**SPPRAMSS-11115, Definition **]**

1.5.4 Reference documentation

A complexity Measure
McCabe,T., IEEE Transactions on software Engineering, Volume SE-2, No. 4, December 1976 **[** Reference, SPPRAMSS-15553 **]**

[IEEE 610.12-1990]
Standard Glossary of Software Engineering Terminology **[** Reference, SPPRAMSS-15551 **]**

Softwarewartung: Grundlagen, Management und Wartungstechniken
dpunkt.verlag, 2016 - Christoph Bommer, Markus Spindler, Volkert Barr **[** Reference, SPPRAMSS-15552 **]**

[EN 50126-1:2017]
Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process **[** Reference, SPPRAMSS-349 **]**

[EN 50126-2:2017]
Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety **[** Reference, SPPRAMSS-335 **]**

[EN 50128:2011 + A2/2020]
Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems

Nota: The standard is superseeded by SPPRAMSS-8814 - [EN 50716:2023], but the SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] does not mention yet the standard. **[** Reference, SPPRAMSS-336 **]**

[EN 50657: 2017/A1:2023]
Railways Applications - Rolling stock applications - Software on Board Rolling Stock
Note: Document will be superseded by prepared EN 50716:2023 **[** Reference, SPPRAMSS-634 **]**

[EN 50129:2018/AC:2019-04]
Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling **[** Reference, SPPRAMSS-334 **]**

[EN 50155:2021]
Railway applications – Rolling stock – Electronic equipment **[** Reference, SPPRAMSS-332 **]**

[EN 50159:2010/A1:2020]
Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems **[** Reference, SPPRAMSS-333 **]**

[EN 61703:2016]
Mathematical expressions for reliability, availability, maintainability and maintenance support terms **[** Reference, SPPRAMSS-4578 **]**

[EN 17023: 2018]
Railway applications - Railway vehicle maintenance - Creation and modification of maintenance plan **[** Reference, SPPRAMSS-9691 **]**

[Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136]
Common Safety Method for risk evaluation and assessment; Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 Text with EEA relevance +
Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment
[Reference, SPPRAMSS-619 **]**

[Directive 2016/797]
DIRECTIVE (EU) 2016/797 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the interoperability of the rail system within the European Union **[** Reference, SPPRAMSS-4525 **]**

[EN 50716:2023]
Railways Applications - Requirements for software development **[** Reference, SPPRAMSS-8814 **]**

[Guidelines for PA VA ERA1209/200 V2.0]
Guide - Guidelines for the practical arrangements for the vehicle authorisation process **[** Reference, SPPRAMSS-8057 **]**

[Commission Implementing Regulation 2023/1695 "TSI CCS"]
Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919 (Text with EEA relevance) **[** Reference, SPPRAMSS-328 **]**

[Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781]
Commission Implementing Regulation (EU) 2020/781 of 12 June 2020 amending Implementing Regulation (EU) 2018/545 as regards the dates of application and certain transitional provisions following the extension of the transposition deadline of Directive (EU) 2016/797 of the European Parliament and of the Council.

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. **[** Reference, SPPRAMSS-327 **]**

[ERA 1209/063 V 1.0]
Clarification Note on Safe Integration
[Reference, SPPRAMSS-9692 **]**

[Decision (EU) 2010/713]
COMMISSION DECISION of 9 November 2010 on modules for the procedures for assessment of conformity, suitability for use and EC verification to be used in the technical specifications for interoperability adopted under Directive 2008/57/EC of the European Parliament and of the Council **[** Reference, SPPRAMSS-9953 **]**

[OCORA release R3]
List of OCORA program deliverables for R3 **[** Reference, SPPRAMSS-9974 **]**

[DMS-ID SA21-00453 - Systemführerschaft ETCS CH]
Systemführerschaft ETCS CH - Sicherheitsnachweiskonzept für die Erlangung einer ETCS-Zulassung in der Schweiz (inkl. Testkonzept) (Fahrzeuge und Infrastrukturanlagen) Version V 3.1 **[** Reference, SPPRAMSS-9983 **]**

SESAMO Project
SESAMO addresses the root causes of problems arising with convergence of safety and security in embedded systems at architectural level, developing a component-oriented design methodology for the safety and security aspects. **[** Reference, SPPRAMSS-9986 **]**

2 State of the art

2.1 Current situation regarding CCS evolutions

Complexity of updating Trackside Elements
For trackside equipment (e.g interlocking, RBC, etc.) it has to be taken into account that equipments are located in different places. Therefore, an installation of new software or hardware substitution implies that personal shall move from one location to another to fulfil these updates, what takes some time: installing new version, checking that version installed is the correct one, restoring equipment service and checking it is done properly, in case of failure they have to be able to re-install the previous version, etc...
[SPPRAMSS-8103, Text **]**

Trackside change management strategy
In case of trackside equipment from a specific project, it has to be configured properly for each location where it is installed. That means that a modification in the generic application has to be validated by the specific project for each location where that equipment is installed. Also it has to be checked that installation of any update has been done properly for each equipment. All that means that Safety Assessor shall review evidences for each location every time a new certification is needed. **[**SPPRAMSS-8104, Text **]**

Railway products life cycle
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 SPPRAMSS-349 - [EN 50126-1:2017]) 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 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 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 SPPRAMSS-327 - [Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781] . This is the mandatory condition for a railway undertaking (or another entity) to use a train on a railway network.
[SPPRAMSS-1006, Text **]**

Safety related systems in the ERTMS environment
Safety related systems in the ERTMS environment (e.g. CCS OB) have to be defined according to the SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]. This considers the technical requirements defined by the different SUBSETS and the CENELEC standards (e.g. SPPRAMSS-349 - [EN 50126-1:2017], SPPRAMSS-8814 - [EN 50716:2023]) plus all the additional standards referred in these three main ones (e.g. SPPRAMSS-7100 - [EN 50159:2010/A1:2020]).
The conformity of the CCS systems 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 SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] 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 system, 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 system. **[**SPPRAMSS-1007, Text **]**

Re-certifications an retro-fits impacts
Over the whole life cycle of a CCS system, new versions of the Safety Case will likely happen several times and the costs related to the re-certification activities are typically very high and for this reason prevent a lot of evolutions which could improve the overall performances of the CCS systems. Indeed, most of the time, the ratio costs vs benefits of the evolutions are not worth realizing it from a business point of view.
The volatility of the CCS system for the railway community is 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) life-cycle. 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. **[**SPPRAMSS-1015, Text **]**

Monolithic approach of the CCS systems
The struggle with retro-fit and re-certification costs happens today because of a monolithic approach of the CCS systems, 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 (e.g. including new hardware). In that case, the CCS system (and thus its safety case(s) and certificate(s)) evolve only by big steps. This is represented in the example on SPPRAMSS-8065 - SUBSET-026 overall vision for ERTMS systems.

[SPPRAMSS-1017, Text **]**

SUBSET-026 overall vision for ERTMS systems

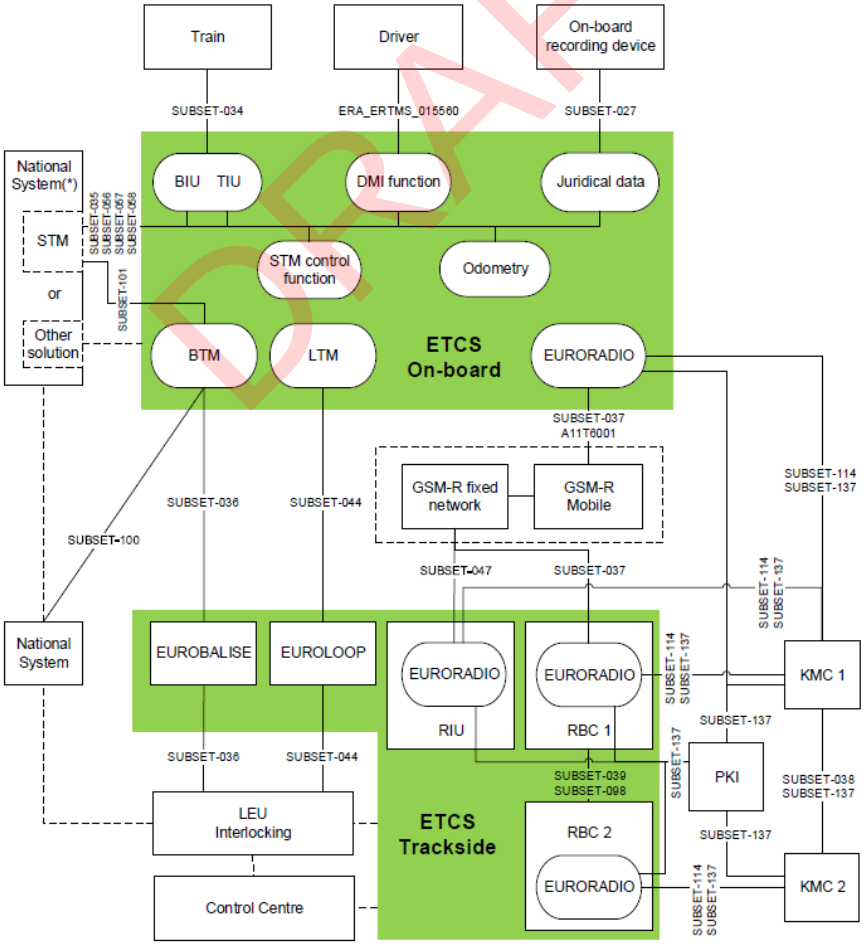


Figure 2 SUBSET-026 overall vision for ERTMS systems

[SPPRAMSS-8065, Diagram **]**

Collect of Change Requests by manufacturers
Manufacturers usually 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 splitting 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 SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]) 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 usually wait months or even years before having their other change requests integrated into a new version of the CCS system. **[**SPPRAMSS-1027, Text **]**

CCS OB example of slow evolutions
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 SPPRAMSS-8065 - SUBSET-026 overall vision for ERTMS systems). 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.

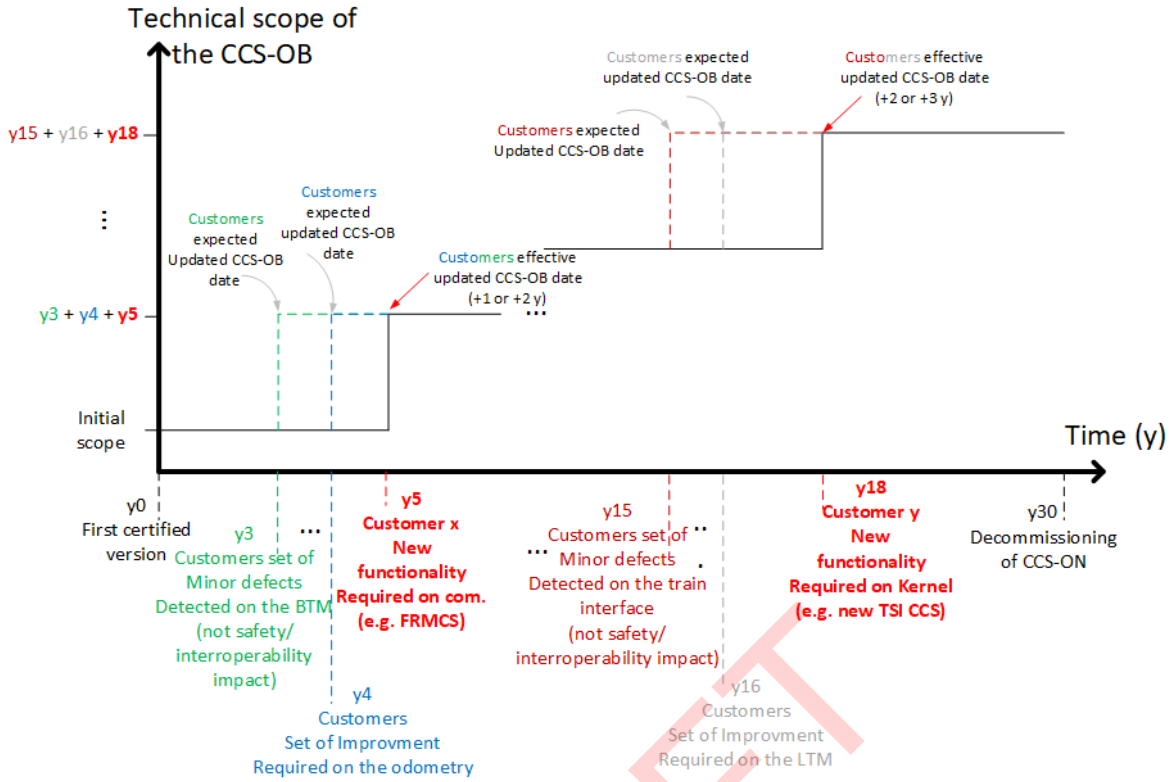


Figure 3 Current example of CCS OB evolution through its life cycle

[SPPRAMSS-1026, Text **]**

2.2 The swiss ETCS implementation as of 2024 - 'Bolli concept'

the swiss ETCS implementation and ERTMS strategy 2023
The standard gauge railway networks in Switzerland are usually equipped with ETCS L1 LS at least, some lines are equipped with ETCS L2. ETCS L2 is operated on key lines of one of the most intensely used railway networks of the planet.
ERTMS activities in Switzerland are steered by the Federal Office of Transport as presented in their ERTMS strategy 2023.
From an authorisation point of view, there is only one area of use in Switzerland, so the interoperability requirements are the same throughout all ETCS equipped lines.
In particular, the Federal Office of Transpor aims at safety regulations which are up to date, appropriate, user friendly, coherent and consistent, economically viable, controllable/enforcable and non discriminative [source: Safety Policy of the Federal Office of Transportation Switzerland - Sicherheitspolitik BAV, BAV-023.11-3/2].
To be able to evolve the ETCS L2 network, an integrated process of approval and authorisation has been adopted, covering the entire system of systems ensuring highly reliable interoperation between the involved trackside and trainborne components, and dealing with issues during operation (life cycle phase 11) as well. This approach is widely known as the 'Bolli concept', named after the main contributor to its invention. **[**SPPRAMSS-10105, Text **]**

The Swiss ETCS implementation: organisational function ETCS System Lead (Systemführerschaft)
The Federal Office of Transport contracts a company of the sector (at present: SBB) to establish an organisation reporting to the Federal Office of Transport (not to the contracted company!) and acting in the function 'Systemführerschaft' (System Lead), which accounts for the steering and control of the implementation of ETCS in Switzerland. Budget, competencies, duties, obligations and targets are defined by the contract.
(Remark: The same concept is applied for trainborne radio, Systemführerschaft Zugfunk is contracted to SBB as well.) **[**SPPRAMSS-8779, Text **]**

The swiss ETCS implementation: reference baseline
The Systemführerschaft defines a 'Bezugskonfiguration' (reference baseline) for the system under consideration in relation to ETCS which contains the requirements to be met by Vehicle Keepers, Railway Undertakings and Infrastructure Managers as defined by the Systemführerschaft. This relates to both, building and operating the system.
The Bezugskonfiguration (reference baseline) consists of a set of documents comprising descriptions and guidelines of binding character going from generic to specific level, including (among else): system description, risk analysis, reference architecture on system level, safety case hierarchy and the related processes.

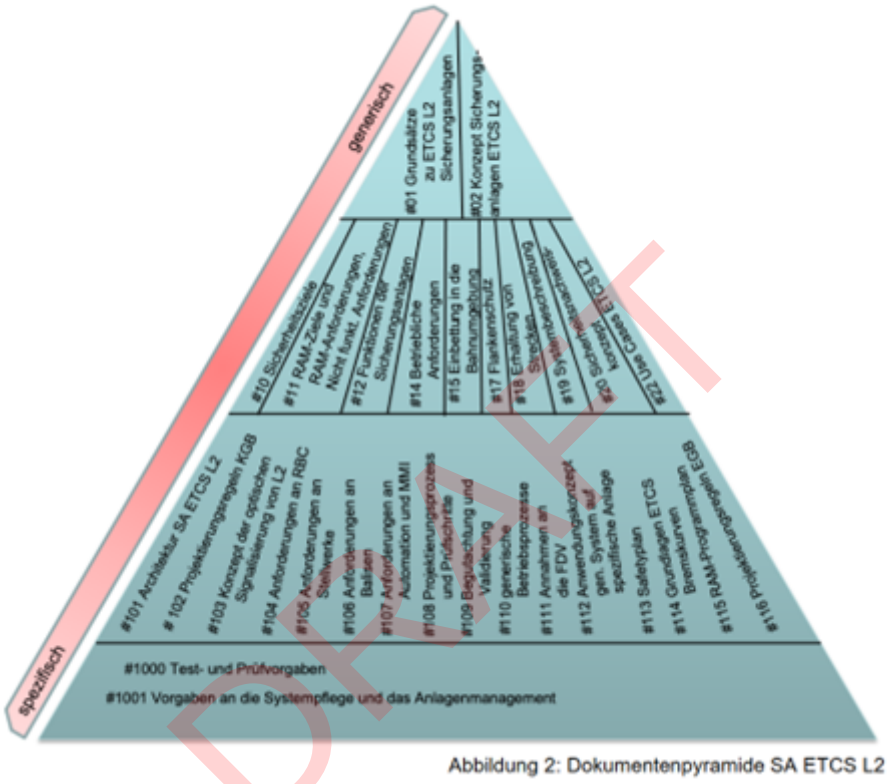


Figure 4 Pyramid of documentation for ETCS L2 projects

The system decribed by the Bezugskonfiguration (reference baseline) is embedded in a system environment as decribed by this figure:

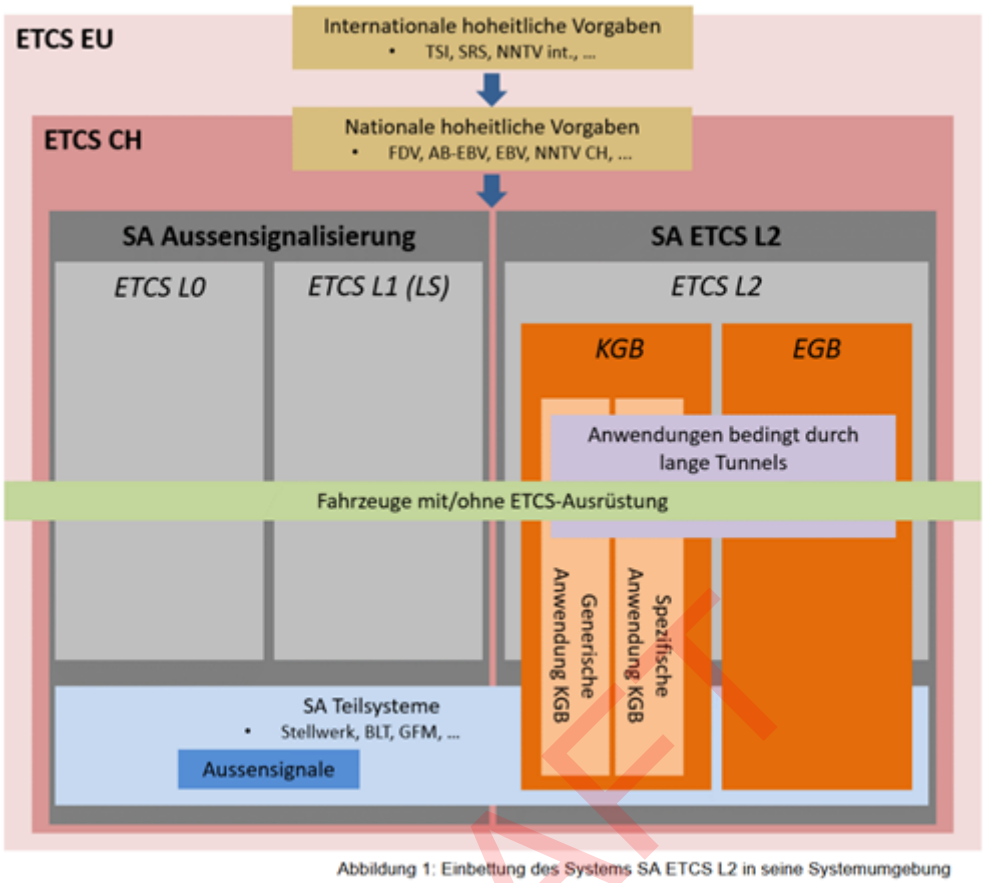


Figure 5 Embedding an ETCS L2 system in its system environment

Table 1 translation of the terms used in the figure

term	translation
Internationale hoheitliche Vorgaben	international regulations
Nationale hoheitliche Vorgaben	national regulation
SA Aussensignalisierung	optical lineside signaling
SA ETCS L2	overall ETCS L2 CCS system
KGB	applications at conventional speed (up to 160km/h)
EGB	applications covering extended speed range
Anwendungen bedingt durch lange Tunnels	applications necessitated by long tunnels
Fahrzeuge mit/ohne ETCS Ausrüstung	vehicles with / without ETCS equipment
Generische Anwendung	generich application
Spezifische Anwendung	specific application
SA Teilsysteme Stellwerk | BLT | GFM || Ausensignale	CCS subsystems interlocking | OCS | train detection || line side signals (optical)

The system under consideration is described by the reference architecture:

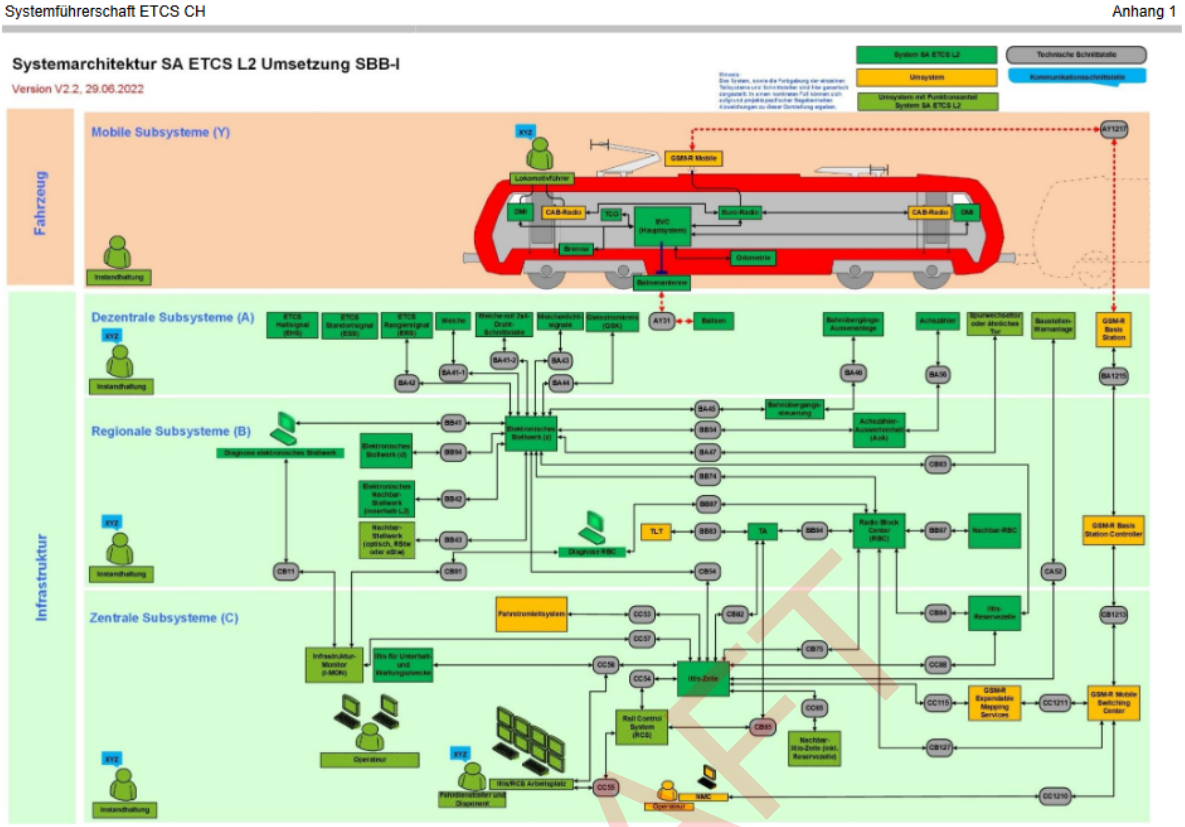


Figure 6 Realisation of an architecture for an ETCS L2 system

Table 2 translation of the terms used for the system architecture components

term	translation
Fahrzeug	vehicle
Mobile Subsysteme	mobile subsystems
Infrastruktur	infrastructure
Dezentrale Subsysteme	decentral subsystems (points, axle counters, etc.)
Regionale Subsysteme	regional subsystems (interlockings, RBCs, etc.)
Zentrale Subsysteme	central subsystems (operations control centre, infrastructure monitoring, etc.)

The result of the process of applying the Bezugskonfiguration is the safety documentation for the overall railway system operating on ETCS in Switzerland. Key features of the chosen approach are:

- Expectations towards each document are described in a section of the concept.
- Risk targets are defined for the overall system, to be able to shift risk acceptance apportionment when necessary.
- As the safety documentation is consolidated into one top level safety case, the safety organisations of the underlying safety cases are part of the overall safety organisation of ETCS in switzerland, and therefore all members of a contributing safety organisation are considered to be member of the overall safety organisation.

Respecting this fact, members of the safety organisation (are required to and do) talk to each other across company / organisational borders to achieve the common goal.

[SPPRAMSS-8778, Text **]**

The swiss ETCS implementation: basic structure of the safety documentation
As the key building blocks of the trackside architecture are provided by different suppliers, a (small) number of top level safety cases (roman numeral I in the following figures), one for each type of the different RBCs, is covering the architecture; while the RBCs and the connected interlockings differ, the structure of these safety cases is the same. Key features of the safety case architecture are:

- to integrally cover trackside installations, vehicles and operation
- to provide generic documents
- to issue operating licenses for vehicles for the entire network (not: line specific)
- to provide the opportunity for specific applications of infrastructure (which need additional Safety Cases) to straightforwardly implement and document (preference of uniform solution over local optimisation is taken care of by plan approval process, etc.)

The basic structure is shown by this figure:

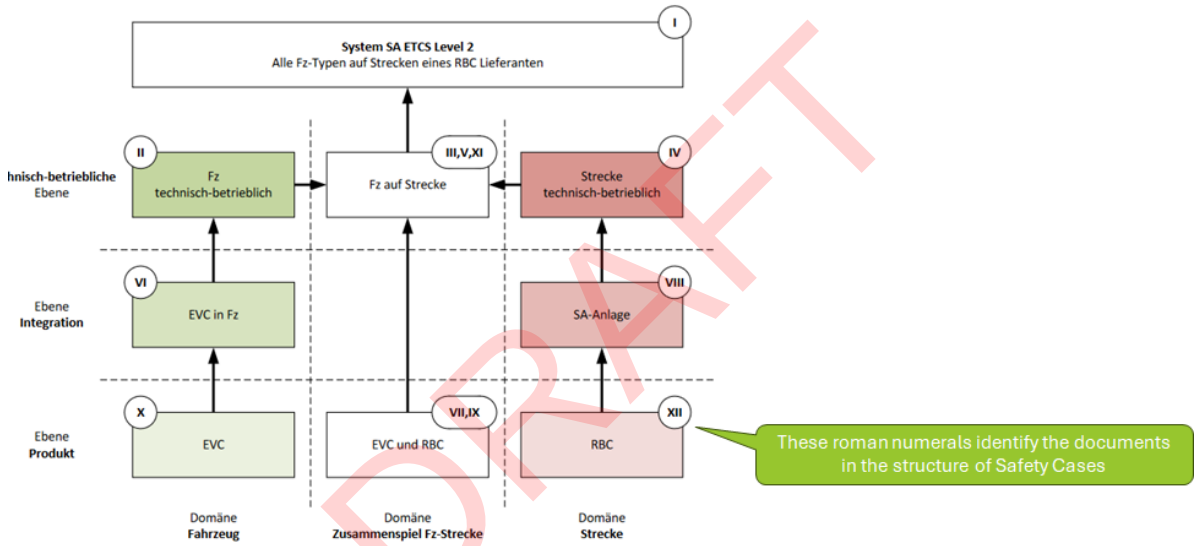


Figure 7 System SA ETCS Level 2

Table 3 translation of the terms used in the above figure

term	translation
alle Fz-Typen auf Strecken eines RBC Lieferanten	all types of vehicles running on lines equipped with RBCs by one RBC vendor
(Fz | Strecke) technisch-betriebliche Ebene	(vehicle | line) technical operational level
Fz auf Strecke	vehicle operated on track of given line
Ebene Integration	integration level
EVC in Fz	EVC integrated into vehicle
SA-Anlage	trackside ETCS CCS system
Ebene Produkt	product level

term	translation
Domäne Fahrzeug	vehicle domain
Domäne Strecke	trackside domain
Domäne Zusammenspiel Fz-Strecke	domain interoperation between vehicle and line

[SPPRAMSS-8781, Text]

The swiss ETCS implementation: safety case structure - dependencies between documents and stakeholders

Obviously, the basic structure depicted in SPPRAMSS-8781 - The swiss ETCS implementation: basic structure of the safety documentation leaves unmentioned all the different relationships between the involved stakeholders, and the respective information flows. The overall documentation will only make proper sense if the interdependencies are respected while planning, developping implementing and documenting the system. It proved advantageous to aim for a set of generic documentation while relating the specific documentation in a defined and controlled way to it. A more detailed view on the safety case structure, including some relevant stakeholders, is given in the following figure (colour code: **Green**: suppliers; **Blue**: infrastructure managers; **Red**: regulator): [SPPRAMSS-8787, Text]

Safety Cases structure in Switzerland

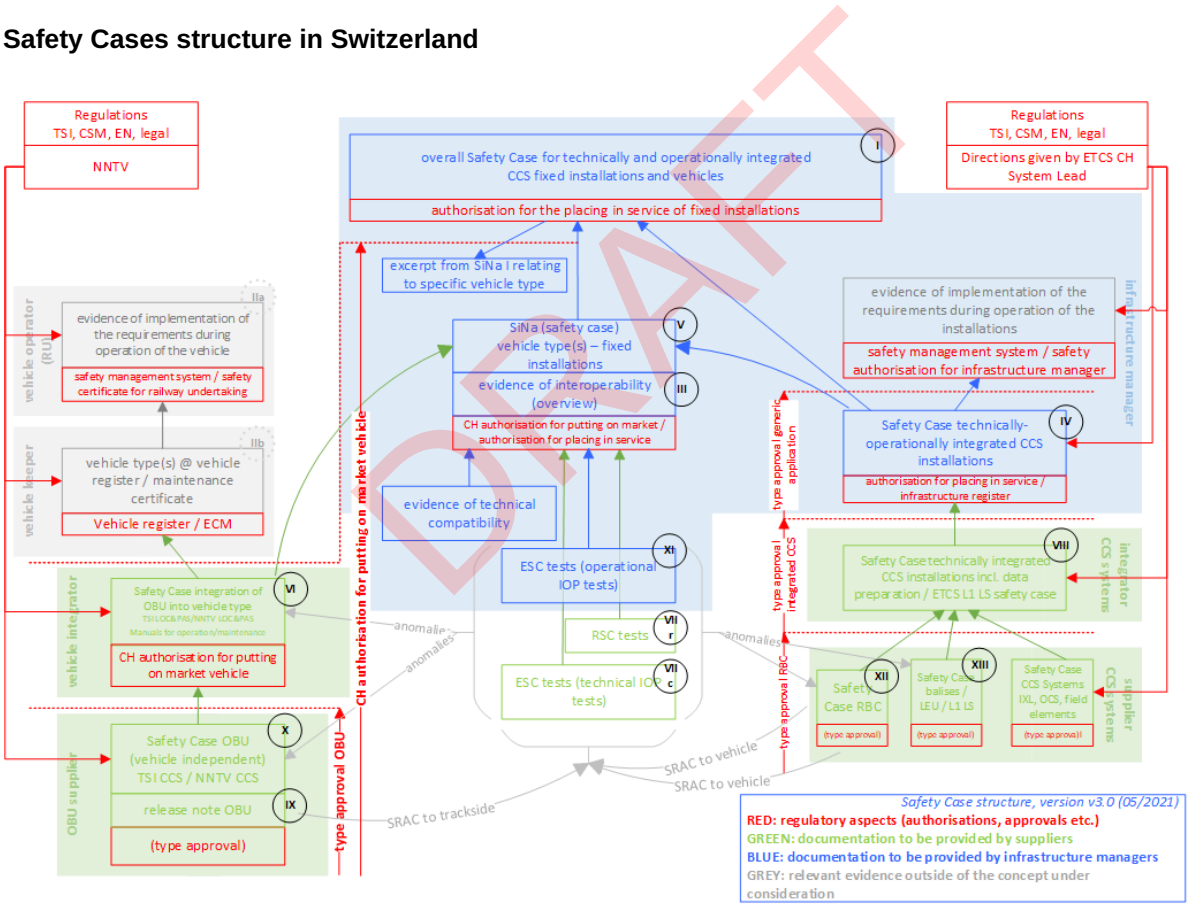


Figure 8 Safety Cases structure (EN) based on SPPRAMSS-9983 - [DMS-ID SA21-00453 - Systemführerschaft ETCS CH]

[SPPRAMSS-9985, Text]

Relations between the generic documents and the Safety Cases

The relations between the generic documents and the Safety Cases for a specific trackside installation are

shown by the following figure:

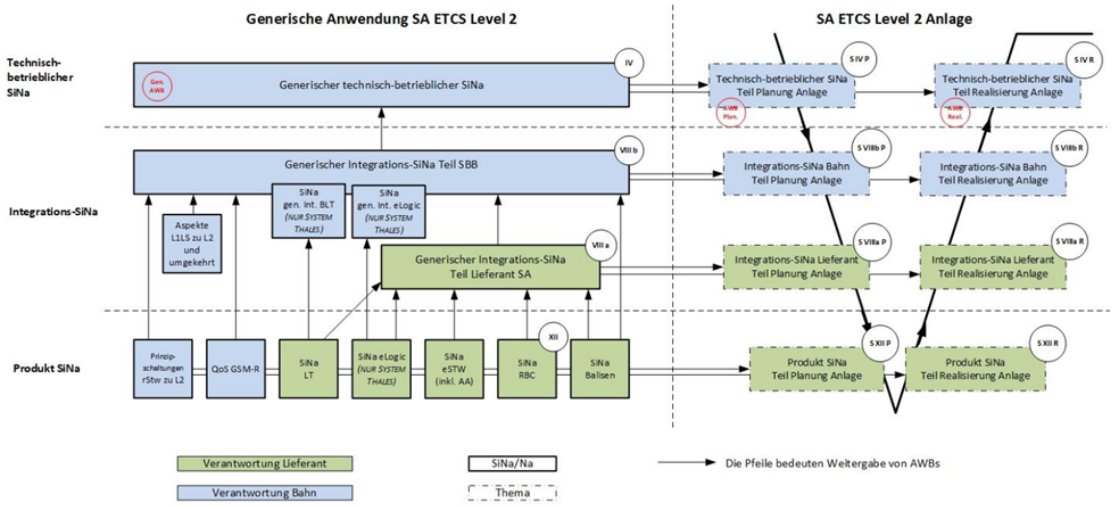


Figure 9 Relation between SiNa Prozess and life cycle

Table 4 translation of the relevant terms used in the figure:

term	translation
Generische Anwendung	generic application
Anlage	installation
Teil SBB	the part contributed by the infrastructure manager integrating the CCS system
Teil Lieferant SA	the part contributed by the supplier(s) of the CCS (sub)system(s)
Verantwortung Lieferant	responsability of the supplier
Verantwortung Bahn	responsability of the infrastructure manager
die Pfeile bedeuten Weitergabe von AWBs	the arrows indicate that SRACs are passed on

[SPPRAMSS-9984, Text **]**

The swiss ETCS implementation: Fundamental rules for the safety cases
Respecting the interdependencies inherent to this approach does not stop at explicating the expected deliverables, their scope and their relationships. More than that, certain expectations must be agreed on and met concerning the content and aim of the safety documentation as well as organisational, information and reporting duties of the involved personnel. This is covered by a set of fundamental rules:

1. The Safety Case of the entire system (roman numeral I), comprising operational and technical aspects and their interdependence, is the basis for vehicle operating licenses.
    - This safety case is always in sole responsability and accountability of the entitiy responsible for the entire system.
    - An operating license is always issued to the vehicle keeper or the concessioned infrastructure manager, nobody else
    - The safety case for the entire system is a necessary precondition for a vehicle operating license
    - The operating license for a vehicle is not issued in relation to a certain line, but always for the entire swiss network

- The concept at hand is intended to clearly allocate responsibilites and accountabilites and to organise the handover of essential information to the higher integration layers, in order to enable working in parallel for the same goal and to understand the chains of dependencies and conclusions that need to be respected
- The Safety Case of the entire system discusses whether, for the safe operation of the entire integrated system and its subsystems, all peripheral necessities, constraints, requirements and preconditions are respected and met, in particular: maintenance handbooks, statements from assessors or NSAs and the like.
  The goal is that operational directives, training documentation and training concepts are properly applicable.

2. The safety documentation shall be derived and maintained for the integrated entire system; the contributing safety cases must respect this to be accepted:

   - Safety Cases must be written according to EN50126-1 and EN50129
   - Safety Cases must take into account and must relate to previously submitted versions of the included documents and their:

     - open/unsolved topics
     - relating documents (if these are of relevance to the new version)
     - assessment reports
     - SRACS
     - subordinated documents' unsolved topics and assessment reports

3. Safety Cases are expected to cover the actual system; they cannot remain unchanged if a substantial circumstance for change is identified. In addition to the judgement of the entity accountable for the Safety Case, sensing a reason for change, this includes:

   - Technical changes: new functionalities, new application data, changes in SRACs or their fulfillment, new purpose of use of the system
   - New insights: changed risk scenario, observed malfunctions or operational deficiencies, intended change of use of the system
   - If a subordinate safety case is changed, it must be checked if this incurs a change of the safety case as well. If so, the change can be taken care of in what is understood to be the most appropriate form: Amendment, new full version, memorandum, etc.
   - In case of substantial changes, a renewed operating license can only be issued after the safety case is completed.
   - For insignificant changes, the safety documentation may be completed and submitted after the renewal of the operating license

4. There are reporting duties which need to be respected:

   - Substantial changes in vehicles must be reported to the Federal Office of Transport. The Federal Office of Transpor decides on the necessity of a (new) operating license
   - Insignificant changes (like bug fixes) do **not** necessitate a (new) operating license.
     Yet the vehicles may only be used after the safety case is completed and all relevant stakeholders are informed
   - For infrastructure systems, the details on the reporting duties are described in a dedicated document.
     Changes in a safety case always need to be indicated to the stakeholders depicted in
     SPPRAMSS-9985 - Safety Cases structure in Switzerland

5. The flow of SRACS as well as the tracing of their fulfillment is controlled by a data base driven tool provided by the Systemführerschaft.

[SPPRAMSS-8780, Text **]**

The swiss ETCS implementation: handling changes and incidents
The structure described so far is easily implementable when building an ETCS system in a green field situation.
Yet one of the major targets of the swiss approach is to be able to efficiently and effectively cope with the

brown field, i.e. an existing ETCS system in operation, facing the necessity for a change:

- Each individual change may be understood as a stimulus to the described structure affecting it initially in one (e.g.: new RBC baseline) or several (e.g.: new radio technology) elements.
  (This is valid for deliberately intended changes bringing enhancements to the overall system just as much as for changes aimed to mitigate incidents in the operation on the network, or reflecting insights gained from such incidents.)
- Simply propagating the stimulus throughout the structure is a straightforward approach:
  - envisioning the change
  - propagating the resulting information to the affected stakeholders authoring the
    - neighbouring documentation and/or
    - next-level documentation,
  - making them aware in time that an updated version of an artefact their documentation refers to
    - is to be expected and
    - will need to be taken care of.
      Where reasonably applicable, this will always be the method of choice.
- However, in many cases this will result in substantial effort involving many people and roles, in unfortunate cases even causing a number of iterations until a satisfying solution is met - in short: Often, this is prohibitively disadvantageous from an economic point of view.

This is why always a way is looked for to minimise the number of affected artefacts, stakeholders and steps:

- Assessment reports:
  A new (release of an) assessment report is necessary in particular if the actual risk situation or the risk evaluation changes or if additional SPPR-3728 - Application Condition are introduced. If a re-assessment does not seem necessary, the author of the safety case has to state the rational for this. The ISA confirms this in a written statement or decides to draft a new (release of the) assessment report.
- Top down view:
  If a change is needed in a more basic part of the document structure, it sometimes is sufficient and appropriate to check from the top from where on else the change has an effect necessary to mention. At that level of documentation (and above), the safety case needs to be updated or amended, all levels in between might be left untouched.
- Bug fixing:
  In particular issues arising during regular operation which are safety relevant or are impairing regular operation to an inacceptable degree exert a high urgency to be fixed. This is why a concerted approach is used in such cases, not only implementing the 'top down view' approach but bringing together all the affected parties as early as possible and balancing the impact across the overall system:
  After all the affected stakeholders have been informed (as appropriate: OBU-/RBC-suppliers, vehicle holders, railway undertakings, infrastructure managers; responsible safety managers, ISAs; the System Lead and the Federal Office of Transpor), an ad-hoc process reflecting the issue under consideration is set up to define the necessary changes and the adequate documentation, approval and authorisation steps.
  The responsibility to conclude the process lies with the vehicle holders (for changes affecting vehicles) and the infrastructure managers (for changes affecting trackside).
  The ad-hoc process comprises at least the following steps:
  - informing all parties affected by the issue under consideration
  - define a project organisation, action plan, documentation plan, rollout plan and time schedule
  - state a problem description and impact analysis (in particular concerning interoperability)
  - specify and then implement the solution
  - document the verification / validation of the solution
  - release the safety case(s), and the ISA's documents according to their involvement (including rationale)

- upgrade the affected systems
- perform the defined measures to supervise the effect of the changes during operation
- mission review of the entire process

Given that all stakeholders are familiar with the Bolli concept and understand the resulting dynamics on the different test and documentation levels, and given that all stakeholders are used to co-operate on solving issues in a balanced way, this approach makes changes viable in a well understood and well controllable way, and in particular urgent changes are possible quickly and effectively. This said, discussions on how to leverage the full potential and improve on cost and time to market are still vivid. **[**SPPRAMSS-10104, Text **]**

The swiss ETCS implementation: important insights

1. The current versions of as well EU legislation as the TSI and the CENELEC standards reflect many of the facets foreseen in the 'Bolli concept', so a lot of the necessary development in the sector to catch up with these current versions may benefit from being inspired by the 'Bolli concept'.
2. A modular architecture cannot be run and evolved successfully without well structured cooperation and coordination between the involved stakeholders.
3. With the coordinated approach at overall system level as defined by the 'Bolli concept', the continuous evolution of the system can be handled well and swiftly, while a number of shortcomings are still obvious:
    a. authorisation is still cost intensive in some cases (room for improvement)
    b. rollout of changes to the field is reasonably viable for trackside installations in general, while changes in track/topology data are still cost and labour intensive due to deficiencies in data flows (no integrated data management for track data between Infrastructure Managers and suppliers)
    c. for trainborne changes rollout to the fleet is impaired by the lack of provisions for efficient update/upgrade/bugfix mechanisms on all sides:
        - in the trainborne products
        - in the maintenance tools and procedures
        - in the fleet management (involving Vehicle Keepers, Railway Undertakings and Entities in Charge of Maintenance)
4. The safety case document structure cannot be copied 1:1 from the 'Bolli concept' to the System Pillar, as it must reflect the underlying system architecture, which in case of the System Pillar is the harmonised reference target architecture. The safety case structure and the necessary interactions between the stakeholders need to be adapted to the System Pillar's reference target architecture if a structure following the ideas of the 'Bolli concept' is intended.
5. The interoperability tests and certificates devised in the TSI are not sufficient to ensure an interoperable overall system (gaps in TSI and CENELEC); additional test facilities and interoperability reports have proven necessary (but with the defined additional reports the set is sufficient)
6. The interface specifications between OBU and RBC are not well defined. While on an international scope, the different operational principles of the railway undertakings and infrastructure managers do not allow for a single RBC product to cover all markets, in the Switzerland-only view the harmonised operation across Switzerland still faces different RBC implementations from the different vendors which individually comply to the TSI but cannot be covered by one overall safety case, as interoperability between vehicles and trackside is not leading to the same overall system behaviour, depending on vehicle/RBC/interlocking integration effects. This is why the top level safety case is instantiated several times, covering one RBC type each.

[SPPRAMSS-10169, Text **]**

Definition of the roles of the different actors

In a next version of the document, the role of the different actors shall be defined, taking inspiration from the Swiss Bolli process, but at a lower level. **[**SPPRAMSS-15557, Issue, Open **]**

2.3 Existing regulations related to evolution management

Analyse that every point is handled by the process
The team shall analyse that every point from SPPRAMSS-1035 - Existing regulations related to evolution management is handled by the process and that there is not conflict between the process and the existing regulations.
This is also connected to the work currently beeing done within the WP26.

For example :

- For Basic Design Characteristics, the consequences of an impact of on the characteristics on the homologation shall be described in the process.

[SPPRAMSS-11465, Issue, Open, Markus Spindler (Rail Expert Consult) **]**

2.3.1 Change management in TSI CCS 2023

2.3.1.1 TSI specifications maintenance process

TSI specifications maintenance process
During the development or operation of subsystems based on the ETCS specification from the TSI CCS, errors or ambiguities may be revealed. These findings are managed as part of the change control procedure under the direction of ERA.
The Railway Agency is responsible for developing the TSI and the ERTMS specification. Regulation 216/796, article 28 clearly defines this mandate. The ERA is in charge of creating guidelines for change requests and managing changes to the ERTMS specifications.
Change requests are created and handled in accordance with the change control management process, for further information see the “procedure Change Control Management PRO_CCM_002 V 2.1”. This process is not changed. This process covers any case of change to the ERTMS specification, while the new process given in the TSI CCS 2023 focus on error prevention normal service.
An example of the compatibility handling for regular changes is given in SPPRAMSS-8055 - Example for ERTMS / ETCS.
However, the change control management process is very extensive and cumbersome. In the event of errors that prevent normal railway operations, a solution must be found immediately. For this purpose, a process for error corrections was defined in Article 10 of TSI CCS (2016/919). The proposed solutions were later published in the form of technical opinions in order to find a standardised solution.
The TSI CCS 2023/1695 (mentioned shortly TSI CCS 2023) introduced a clear section defining a specification maintenance process to deal with errors preventing normal railway service.
A main key change is the legally binding of a change and its implementation within the interoperability constituents (trackside or on-board). In the past, emergency changes (error changes where article 10 applies) to the specification were published by ERA as a Technical Opinion in accordance with Article 10 (TSI CCS 2016/919). In accordance with the referenced Article 10, a Technical Opinion can be regarded as transitional documentation if no immediate revision of the specification is necessary. This means that a technical opinion is not legally binding. Compared to that the TSI 2023 defines requirements giving a clear transition period to implement the error corrections published in a next version of the TSI CCS.
The following figure shows an interpretation of the process according to chapter 7.2.10 of TSI CCS 2023 and summerises it, SPPRAMSS-7350 - 7.2.10. Specifications maintenance (error corrections).

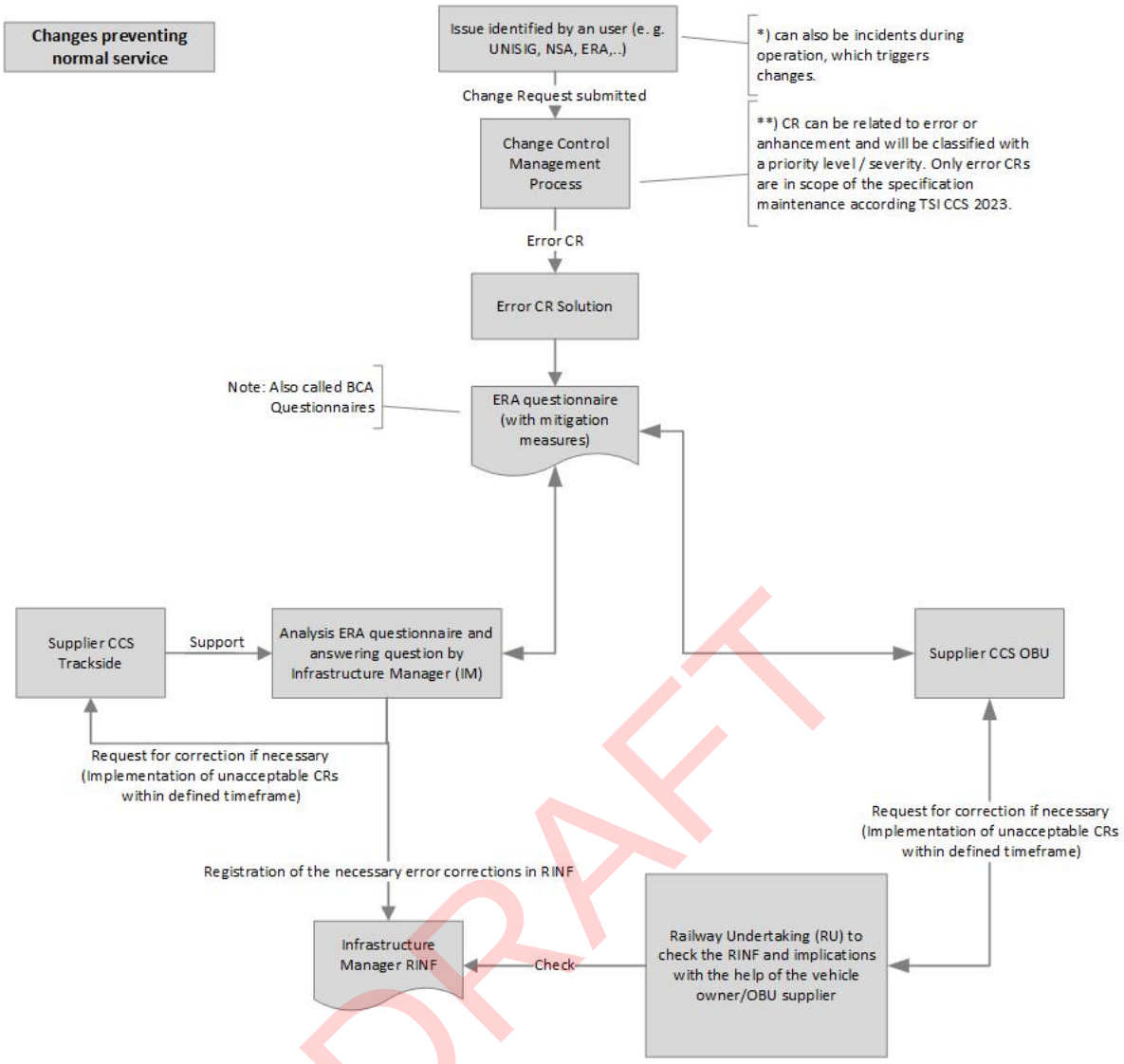


Figure 10 Process - Changes preventing normal service

Chapter 7.2.10.2 in TSI 2023 states that after the publication of the error corrective / solution in a legal version (update of the specification/TSI CCS), the interoperability constituents must be updated by the manufacturers.
The infrastructure manager must specify in the RINF characteristics which corrective actions are necessary for the on-board subsystem on its line no later than 12 months after the TSI comes into force. The railway undertaking must check the RINF and have the necessary corrective actions carried out within the timeframe given in TSI CCS 2023 table B3.
The following points can be summerized:

- It can be stated that the process for changing the specifications is complex and offers room for interpretation. Different handling can lead to unnecessary costs.
- The implementation of error corrections that lead to the adaptation of the specifications becomes legally binding via an amendment to the TSI.
- An infrastructure manager must document error corrections that prevent normal operation in the RINF. The manufacturers are obliged to make corrections.

Potential for future improvements is seen in the following aspect:

- The question of how the financial costs are distributed among the stakeholders has not yet been answered. It should be noted that the originators of an error CR are not necessarily the

actors who ultimately have to implement the solution. With reference to the legal obligation to implement the CRs listed in the future TSIs CCS, it would be desirable to establish a mechanism to distribute the costs incurred in an appropriate manner.

[SPPRAMSS-10103, Text **]**

Example for ERTMS / ETCS
ERTMS / ETCS is designed to ensure interoperability and compatibility between the different subsystems across Europe's rail network. Several mechanisms are in place to ensure compatibility.
ERTMS/ETCS is developed based on well-defined requirement baselines. Each version introduces improvements, updates or error corrections. These evolutions are embedded within a baseline version mentioned within the TSI CCS. For example, the TSI CCS (2016/919) defines three sets of specifications:

- Set of Specification #1 for ETCS Baseline 2 and GSM-R Baseline 1,
- Set of Specification #2 for ETCS Baseline 3 Maintenance Release 1 and GSM-R Baseline and
- Set of Specifications #3 for ETCS Baseline 3 Maintenance Release 2 and GSM-R Baseline 1.

Note: The TSI CCS 2023 lists just one set of specification containing the ETCS baseline 4 release 1, GSM-R Baseline 1 Maintenance Release 1 + FRMCS Baseline 0 and ATO Baseline 1 Release 1.

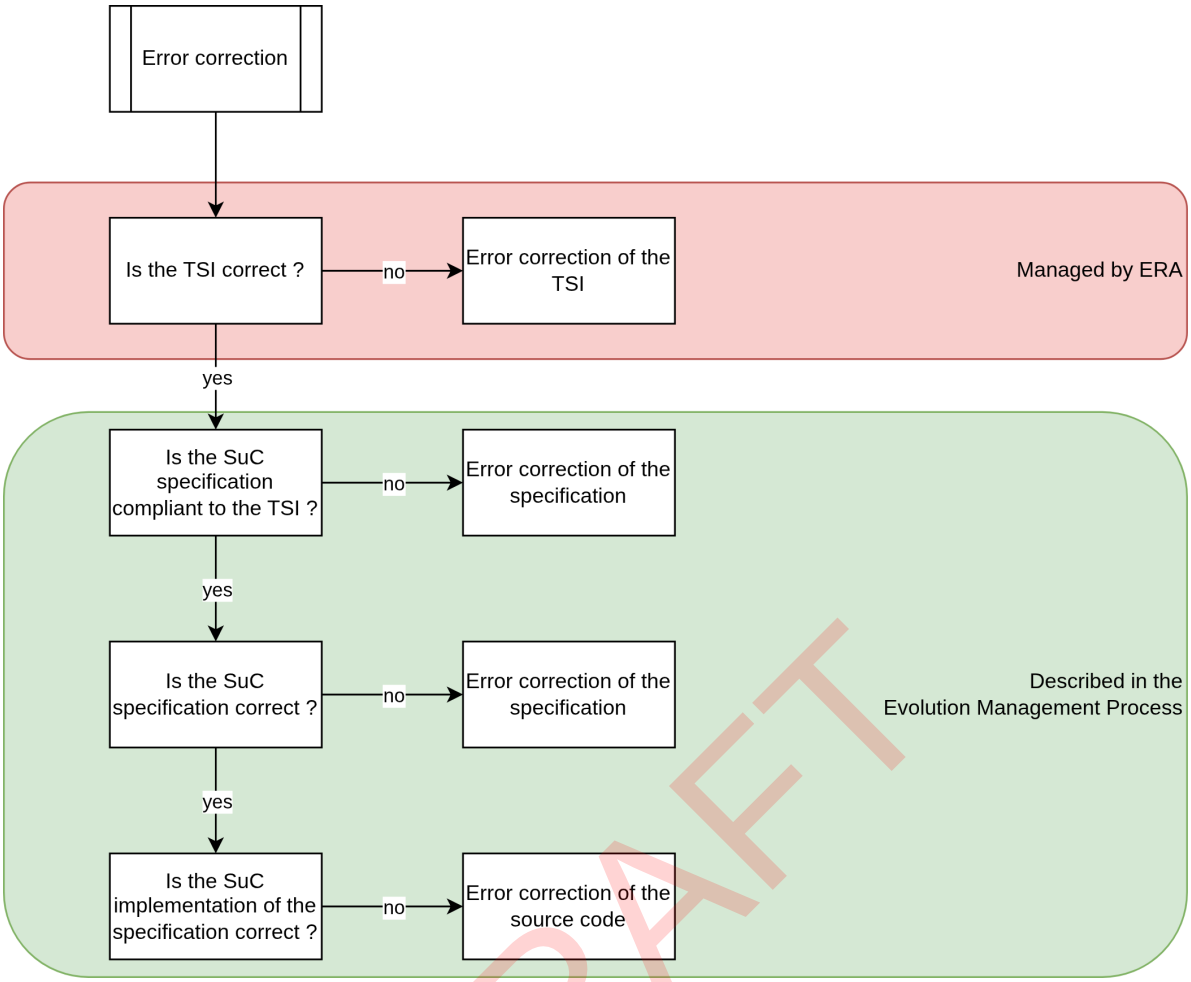
To ensure compatibility between subsystems, it is necessary to adhere to the same baseline version of the ERTMS/ETCS specification.
Change requests (CRs) are used to update the specification due to improvements or errors.
An analysis is undertaken between major releases containing all CRs introduced into a new baseline version to ensure conformity. The results are documented in a Baseline Compatibility Analysis (BCA) report. The results of the Baseline compatibility assessment process for each individual change identified by a change request (CR) are shown, with regards to backwards compatibility.
The M_Version variable for system version, as defined in Subset-026-7.5.1.79, v340, is crucial for ensuring compatibility between different subsystems. It follows the format X.Y, where the first number distinguishes incompatible versions and the second number indicates compatibility within a version. A management of older system versions is defined archive backwards compatibility.
The set of specification and the system version is part of the TSI certificate.
Conformity Assessment procedures verify that ETCS onboard units and trackside subsystems comply with relevant ERTMS/ETCS specifications. **[**SPPRAMSS-8055, Text **]**

2.3.1.2 Error correction at building block level

Error correction
The chapter 6.5 "Management of errors" of SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] describes the process to apply an error correction.

Error corrections are a type of evolutions, covered by the Evolution management process. Several types of error correction at building block level can occur:

- error correction of the TSI, because it is incorrect (curently not covered by the Evolution Management process).
- error correction of the specification, because it is not compliant with the TSI.
- error correction of the specification, because it is incorrect
- error correction of the source code, because it is not implementing correctly the specification i.e. "deviating from intended functions and/or performance".



[SPPRAMSS-14396, Text]

2.3.1.3 Basic design characteristics and basic parameters

Clarification on wording
From document SPPRAMSS-8057 - [Guidelines for PA VA ERA1209/200 V2.0] :
It is important to differentiate between the terms used to describe the parameters for vehicles i.e. “basic design characteristics” and “basic parameters”:

- Basic design characteristics are defined in Article 2(2) of **SPPRAMSS-327 - [Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781]:**
  - *(2) ‘basic design characteristics’ means the parameters that are used to identify the vehicle type as specified in the issued vehicle type authorisation and recorded in the European Register of Authorised Vehicle Types (‘ERATV’).*
- “Basic parameters” are defined in Directive (EU) 2016/797 Article 2(12) as ”any regulatory, technical or operational condition which is critical to interoperability and is specified in the relevant TSIs”.

The basic parameters covered by TSIs are those that need to be harmonised to meet the objectives of Directive (EU) 2016/797. This includes the parameters necessary to ensure technical compatibility between vehicle and network, and their values. For each basic parameter, the requirement(s) are defined either through a TSI rule or through a national rule (e.g. open point in the TSI). These should be checked by the NoBo/ DeBo before the authorisation, as required by the relevant TSIs and/ or national rules.

[...]
The basic design characteristics for a vehicle type are a result of the combination of the parameters of the subsystems of which it is composed and their interaction when integrated into a vehicle design. The TSIs identify the parameters that require harmonisation for interoperability; other aspects of the vehicle's design that are not harmonised may also be considered as basic design characteristics.
[...]
At the time of publication of this guideline, the basic design characteristics account are those referred to in **SPPRAMSS-8138 - Article 48(c) of Commission Implementing Regulation 2018/545**.
[SPPRAMSS-8056, Text **]**

Article 48(c) of Commission Implementing Regulation 2018/545
Article 48
The information in the issued vehicle type authorisation
[...]

- (c) an identification of the **basic design characteristics** of the vehicle type:
  - (i) stated in the type and/or design examination certificates;
  - (ii) the area of use of the vehicle;
  - (iii) the conditions for use of the vehicle and other restrictions;
  - (iv) the reference, pursuant to the provisions of Article 16 of Regulation (EU) No 402/2013, including the document identification and the version, to the written declaration by the proposer referred to in Article 3(11) of Regulation (EU) No 402/2013, covering the vehicle type

[SPPRAMSS-8138, Text **]**

Basic parameters
The *basic parameters* mentioned in Table 4.1 of SPPRAMSS-7339 - 4.1.3. Parts of Control-command and Signalling Subsystems refer to the *list of mandatory specifications* for the *ERTMS Baseline 4 Release 1* as presented in SPPRAMSS-8048 - Link between basic parameters and mandatory specifications . This means that *basic parameters* refers to all ERTMS technical specifications (e.g. SUBSETs) including the safety related SUBSET (i.e. SUBSET-091). The application of the CENELEC standards is called in section SPPRAMSS-7320 - 4.2.1.1. Safety and therefore, is part of the *basic parameters*.
[SPPRAMSS-8050, Text **]**

6.1.1.1. Compliance with basic parameters
Fulfilment of the essential requirements set out in Chapter 3 [THE ESSENTIAL REQUIREMENTS FOR THE CONTROL-COMMAND AND SIGNALLING SUBSYSTEMS] of this TSI shall be ensured through compliance with the basic
parameters specified in Chapter 4 [CHARACTERISATION OF THE SUBSYSTEMS].
This compliance shall be demonstrated by:
(1) assessing the conformity of the interoperability constituents specified in Chapter 5 (see points 6.2.1, 6.2.2, 6.2.3, 6.2.4);
(2) verifying the subsystems (see point 6.3 and point 6.4).
In case of **changes** to existing subsystems, the requirements in **7.2.2** for on-board subsystems and **7.2.3** for trackside
subsystems shall be considered in the assessment. **[**SPPRAMSS-7324, Text **]**

4.1.3. Parts of Control-command and Signalling Subsystems
According to point 2.2 (Scope) the Control-Command and Signalling Subsystems can be subdivided in parts.

The following table indicates which **basic parameters** are relevant for each subsystem and for each part.

Table 4.1

Subsystem	Part	Basic parameters
Control-Command and Signalling On-board	Train protection	4.2.1, 4.2.2, 4.2.5, 4.2.6, 4.2.8, 4.2.9, 4.2.12, 4.2.14, 4.2.16
	Voice radio communication	4.2.1.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.13, 4.2.16
	Data radio communication	4.2.1.2, 4.2.4.1, 4.2.4.3, 4.2.5.1, 4.2.6.2, 4.2.16
Control-Command and Signalling Trackside	Train protection	4.2.1, 4.2.3, 4.2.5, 4.2.7, 4.2.8, 4.2.9, 4.2.15, 4.2.16
	Voice and data radio communication	4.2.1.2, 4.2.4, 4.2.5.1, 4.2.7, 4.2.16
	Train detection	4.2.10, 4.2.11, 4.2.16

[SPPRAMSS-7339, Text **]**

Link between basic parameters and mandatory specifications
Example with: **4.2.10. Trackside Train Detection Systems**
This basic parameter specifies the interface requirements between the trackside train detection systems and rolling stock, related to vehicle design and operation.
The interface requirements to be respected by the train detection systems are specified in **Appendix A, Table A 1, 4.2.10 a**.

Appendix A ([41])

References

For each reference made in the basic parameters (point 4 of this TSI) the following table indicates the corresponding mandatory specifications, via the Index in Table A 2.

Table A 1

References between basic parameters and mandatory specifications

Reference in Chapter 4	Index number (see Table A 2)
...	
4.2.10	
4.2.10 a	77 (point 3.1)

Table A 2

List of mandatory specifications

Index No	ETCS Baseline 4 Release 1; RMR: GSM-R Baseline 1 Maintenance Release 1 + FRMCS Baseline 0; ATO Baseline 1 Release 1			
	Reference	Name of Specification	Version	Notes
...				
77	ERA/ERTMS/033281	Interfaces between CCS trackside and other subsystems	5.0	Note 6

SUBSET-077 v5.0: ERA ERTMS/ETCS UNIT -

Interfaces between Control-Command and signalling trackside and other susbsystems

3. INTERFACE CHARACTERISTICS

3.1. VEHICLE DESIGN AND OPERATION

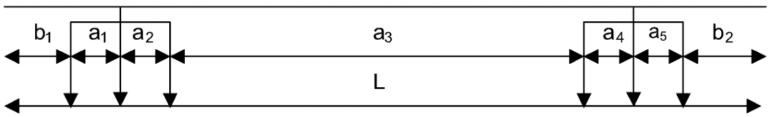
3.1.1. Definitions

For the definition of the longitudinal vehicle dimensions Figure 1, (which shows an example for a three-axle twin-bogie vehicle), applies, where:

a_i = distance between following axles, where i = 1, 2, 3, …, n-1, where n is total number of axles of the vehicle

b_x = distance from first axle (b_1) or last axle (b_2) to the nearest end of the vehicle, i.e. nearest buffer/nose

L = total length of the vehicle



[SPPRAMSS-8048, Text]

2.3.1.3.1 CCS-OB basic design characteristics

Table 7.1.Basic Design Characteristics

1. TSI Point	2. Related basic design characteristic(s)	3. Changes not impacting the basic design characteristics according to 15(1)(b) of Implementing Regulation (EU) 2018/545	4. Changes impacting the basic design characteristic but inside the acceptable range of parameters therefore to be classified as Art 15.1(c) of Implementing Regulation (EU) 2018/545	5. Changes impacting the basic design characteristic and outside the acceptable range of parameters therefore to be classified as Art 15.1 (d) of Implementing Regulation (EU) 2018/545
4.2.2 On-Board ETCS functionality	ETCS equipment on-board and the set of specification of CCS TSI Appendix A	Not applicable	Not applicable	Use another Appendix A set of specifications.
	Envelope of legally operated ETCS system versions	Not applicable	Not applicable	Installation or start the operational use of ETCS; Modification of the envelope of legally operated ETCS system versions from set of specifications in Appendix A.
	ETCS On-board implementation	Fulfilling all the conditions in point 7.2.2.2 (change of realisation identifier)	Not applicable	Not fulfilling all the conditions in point 7.2.2.2 (change of functional identifier)
	Managing information about the completeness of the train (not from driver)	Not applicable	Adding or removing train integrity supervision	Not applicable
	Safe consist length information from on-board necessary to access the line and SIL	Not applicable	Adding or removing safe consist length information	Not applicable
4.2.17.1 ETCS System Compatibility	ETCS System Compatibility	Not applicable	Adding or removing an ESC statement fulfilling all the conditions in point 7.2.2.4.	Adding or removing an ESC statement not fulfilling all the conditions in point 7.2.2.4.
4.2.4 Mobile communication functions for railways RMR 4.2.4.2.1 GSM-R Voice and operational communication applications	GSM-R Radio voice on board and its Baseline	Usage of another Baseline fulfilling all the conditions in point 7.2.2.3	Not applicable	Installation or start the operational use of GSM-R cab radio; Usage of another Baseline not fulfilling all the conditions in point 7.2.2.3.
	GSM-R Voice and operational communication implementation	Fulfilling all the conditions in point 7.2.2.3 (change of realisation identifier)	Not applicable	Not fulfilling all the conditions in point 7.2.2.3 (change of functional identifier)
	GSM-R Voice SIM Card support of Group ID 555	Not applicable	Change the SIM Card support of Group ID 555	Not applicable
4.2.17.3 ETCS and Radio System Compatibility	Radio Voice System Compatibility	Not applicable	Adding or removing an RSC statement fulfilling all the conditions in point 7.2.2.4.	Adding or removing an RSC statement not fulfilling all the conditions in point 7.2.2.4.
4.2.4 Mobile communication functions for railways RMR 4.2.4.3.1.1 GSM-R data communication for ETCS 4.2.4.3.2.1 GSM-R data communication for ATO	GSM-R Radio Data communication on board and its Baseline	Usage of another Baseline fulfilling all the conditions in point 7.2.2.3.	Not applicable	Installation or start the operational use of GSM-R EDOR; Usage another Baseline not fulfilling all the conditions in point 7.2.2.3.
	GSM-R Data communication for ETCS and ATO implementation	Fulfilling all the conditions in point 7.2.2.3 (change of realisation identifier)	Not applicable	Not fulfilling all the conditions in point 7.2.2.3 (change of functional identifier)
4.2.17.3 ETCS and Radio System Compatibility	Radio Data System Compatibility	Not applicable	Adding or removing an RSC statement fulfilling all the conditions in point 7.2.2.4.	Adding or removing an RSC statement not fulfilling all the conditions in point 7.2.2.4.
4.2.4 Mobile communication functions for railways RMR 4.2.4.1.1 GSM-R Basic communication function	Voice SIM Card GSM-R Home Network	Not applicable	Replacement of a TSI compliant GSM-R SIM Card by another TSI compliant GSM-R SIM Card with a different GSM-R Home Network	Not applicable
	Data SIM Card GSM-R Home Network	Not applicable	Replacement of a TSI compliant GSM-R SIM Card by another TSI compliant GSM-R SIM Card with a different GSM-R Home Network	Not applicable
4.2.18 On-Board ATO functionality	On-board ATO system version	Not applicable	Change of the ATO system version fulfilling all the conditions in point 7.2.2.3.	Add or remove the ATO part of the CCS on-board subsystem; Start the operational use of ATO. Or change of the ATO system version not fulfilling all the conditions in point 7.2.2.3.
	On-board ATO implementation	Fulfilling all the conditions in point 7.2.2.3 (change of realisation identifier)	Not applicable	Not fulfilling all the conditions in point 7.2.2.3 (change of functional identifier)
7.2.5 Legacy systems	Class B or other train protection, control and warning legacy systems installed (system and, if applicable, version)	The requirements for Class B system are the responsibility of the relevant Member State.	The requirements for Class B system are the responsibility of the relevant Member State.	Add or remove Class B train protection systems. The requirements for Class B system are the responsibility of the relevant Member State.
	Class B or other radio legacy systems installed (system and, if applicable, version)	The requirements for Class B system are the responsibility of the relevant Member State.	The requirements for Class B system are the responsibility of the relevant Member State.	Add or remove Class B radio legacy systems. The requirements for Class B system are the responsibility of the relevant Member State.

[SPPRAMSS-7340, Text]

2.3.1.3.2 CCS-TRK basic design characteristics

Table 7.2. - Trackside basic parameters modifications which requires a new authorisation

Basic Parameter		Modification which requires a new authorisation
4.2.3	Trackside ETCS functionality	Not fulfilling all the conditions in point 7.2.3.2
4.2.4 4.2.4.2	Mobile communication functions for railways RMR Voice and operational communication applications	Not fulfilling all the conditions in point 7.2.3.3
4.2.4 4.2.4.3	Mobile communication functions for railways RMR Data communication applications for ETCS and ATO	Not fulfilling all the conditions in point 7.2.3.3
4.2.19	Trackside ATO functionality	Not fulfilling all the conditions in point 7.2.3.3

[SPPRAMSS-8047, Text **]**

2.3.1.4 Change management in CCS systems depending on the change type

Different type of changes
SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] specifies different type of change management in case they are impacting or not the *basic parameters* (SPPRAMSS-7339 - 4.1.3. Parts of Control-command and Signalling Subsystems) / *basic design characteristics* (SPPRAMSS-7339 - 4.1.3. Parts of Control-command and Signalling Subsystems for OB and SPPRAMSS-8047 - Table 7.2. - Trackside basic parameters modifications which requires a new authorisation).

This distinction of these different set of activities depending of the type of change will strongly influence the strategy of separation of items in SP. This will be defined later in the document. **[**SPPRAMSS-8049, Text **]**

Changes that do not impact the basic parameters / basic design characteristics
The major change from previous TSI CCS is that from now, the document clearly specifies types of changes that do not impact the basic parameters / basic design characteristics and therefore do not impact the assessment performed on the system (i.e. ISA, NoBo). These types of changes are identified in:

- SPPRAMSS-7345 - 7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics
- SPPRAMSS-8058 - 7.2.2.3 Conditions for a change in the On-board mobile communication functions for railways or in the ATO on-board functionality that does not impact the basic design characteristics
- SPPRAMSS-8061 - 7.2.2.4 Conditions for a change in the on-board...
- SPPRAMSS-8078 - 7.2.3.1 Rules to manage or renewal of existing trackside CCS subsystems
- SPPRAMSS-8080 - 7.2.3.2 Conditions for an upgrade or renewal in the trackside ETCS functionality that, if not fulfilled, requires new authorisation for placing in service
- SPPRAMSS-8082 - 7.2.3.3 Conditions for an upgrade or renewal in the trackside mobile communication for railways or trackside ATO functionality that, if no fulfilled, requires a new authorisation for placing in service
- SPPRAMSS-8081 - 7.2.3.4 Impact o the technical compatibility between on-board and trackside parts if the CCS subsystems

[SPPRAMSS-8052, Text **]**

7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics

(1) The target functionality ([17]) remains unchanged or is set to the state already expected during the original
certification or authorisation. Target functionality is **considered unchanged when applying the specification**
maintenance (error correction) process described in point SPPRAMSS-7350 - 7.2.10. Specifications maintenance (error corrections) which includes the implementation of error corrections or the implementation of mitigation measures.

([17]) Target functionality refers to the ETCS functionality that has been evaluated in the subsystem EC certificate. The Technical Opinions published by the Agency that correct errors in the TSI are considered to define the functionality state already expected during the original certification or authorisation.

=> Clarification: no ERTMS relevant functionality shall be impacted by the change (i.e. linked to *basic parameters*). The only possibility to change them is in case of retro-fit of product, it shall be put in the same previous status as the last valid NoBo certification.

=> This should require a strict separation between ERTMS functionalities and non-ERTMS functionalities.

=> Section SPPRAMSS-7350 - 7.2.10. Specifications maintenance (error corrections)deals with maintenance into TSI documentation (e.g. Subsets) in case of errors into the interoperability specifications.

=> Would a strict separation between different ERTMS functionalities be relevant to mitigate the impact of rework/reassessment in case of specification maintenance?

(2) The **interfaces** relevant for **safety & technical compatibility** remain **unchanged** or are set to the state already
expected during the original certification or authorisation.

=> Clarification: no ERTMS relevant interface shall be impacted by the change (i.e. linked to *basic parameters*). The only possibility to change them is in case of retro-fit of product, it shall be put in the same previous status as the last valid NoBo certification.

(3) The **result of the safety judgement (e.g. safety case according to EN 50126) remains unchanged.**

=> Clarification: no safety mechanism can be changed without a new reassessment.

=> This should require a strict separation between safe and non-safe functionalities.

=> Thanks to a segregation mechanism, the safety case of each building block will highlight which parts are safe (i.e. SIL 1 to SIL4) and which ones are BIL. Then, only the modifications in a safe part would lead to impact the last certification status (which relies on the conclusion of the methodology defined in SPPRAMSS-5670).

(4) **No new** safety related application conditions (**SRAC**) **or interoperability constraints** have been added due to the
change.

=> Clarification: the PRAMS team shall attention to the fields letting space to add SRAC in the SP architecture (e.g. maintenance, installation) as they have a direct impact on the smooth evolvability of the Building Blocks.

(5) A **CSM assessment body** (CSM RA) as specified in point 4.2.1 (=> SPPRAMSS-7320 - 4.2.1.1. Safety and SPPRAMSS-7375 - 4.2.1.2 Availability/Reliability) has independently **assessed** the applicant's risk assessment and within it the **demonstration that the change does not adversely affect safety**. The applicant's demonstration shall include the evidence that the **change** actually corrects the causes of the initial deviation of the functionality.

=>Clarification: not sure to clearly understand the difference with (3) since now in TSI CCS 2023 CSM body replaces ISA (refer to SPPRAMSS-7320 - 4.2.1.1. Safety)

(6) Depending on the type of **change**:

- (a) in the case where the **change** is made due to a product error: The change is performed under a quality management system approved by a notified body. For other modules it shall be justified that the verification performed remains valid ([18]);

=> Clarification: this refers to bugs, failures, weaknesses of the products and are product specific. This shall a topic to be handled by the Evolution Management process.

([18]) All activities required for a modification which are performed outside a quality management system approved by a notified body might require additional examinations or tests by the notified body.

- (b) in the case where the **change** is made due to the specification maintenance process (there are updated specifications in Appendix A Table A 2 with the descriptions of the error correction): an updated EC design examination or EC type examination certificate for the Interoperability Constituents or Subsystem with the implementation of error corrections is needed. In this case the provisions of point 6.3.3 (3) apply (=> SPPRAMSS-7385 - 6.3.3. Assessment requirements for an On-board Subsystem).
  => Clarification: this refers to errors due to TSI/Subsets specifications errors (i.e. SPPRAMSS-7350 - 7.2.10. Specifications maintenance (error corrections). It concerns all products, independently from the manufacturer. The Evolution Management process shall analyse if proposer additional separation (i.e. between ERTMS functionalities) can help at dealing with this point.

(7) The individual configuration management defines a 'system identifier' (as defined in 4.2.20.3) and the
'functional identifier' of the 'system identifier' has not been changed after the **change**.
=> Clarification: the PRAMS team shall propose a strategy to harmonise the 'system identifier' for all building blocks and integrated systems. This shall be done in collaboration with the Task 2 - Transversal - SD3 working group.

(8) The **change** shall be part of the configuration management required by Article 5 of SPPRAMSS-327 - [Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781] . (=> SPPRAMSS-7390 - Commission Implementing Regulation 2018/545 - Article 5)
=>Clarification: the changes shall be visible from building block configuration to the complete vehicle type configuration (to be pushed later in Transversal domain). The Evolution Management process (or another PRAMS document) shall also take care of the propagation of errors from building blocks until full vehicle (i.e. trackside in not considered by SPPRAMSS-327 - [Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781] . **[**SPPRAMSS-7345, Text **]**

2.3.1.5 Safety requirements for change management in CCS systems

Separation rules in the building blocks
In order to improve evolvability, a strict separation (i.e. as presented in SPPRAMSS-334 - [EN 50129:2018/AC:2019-04]) shall be implemented in any building block according to the following list:

- SIL1 to SIL4 and interoperable functions
- BIL and interoperable functions
- SIL1 to SIL4 and non-interoperable functions
- BIL and non-interoperable functions
- Cyber-security functions

ID	SPPRAMSS-1150
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Rationale - Separation rules in the building blocks
From a certification point of view, no separation rules between safe and basic parameters elements is mandatory as primary requirement as any modification on one of this item lead to a new NoBo certification (refer to SPPRAMSS-7345 - 7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics or SPPRAMSS-8080 - 7.2.3.2 Conditions for an upgrade or renewal in the trackside ETCS functionality that, if not fulfilled, requires

new authorisation for placing in service).
Additional separation rules may be defined once the overall modular architecture of the CCS systems is defined (i.e. in Phase 5 as defined in PRAMS Plan).

The figure below illustrates the reasons for requiring strict sepration between different type of functions within the frame of SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"].

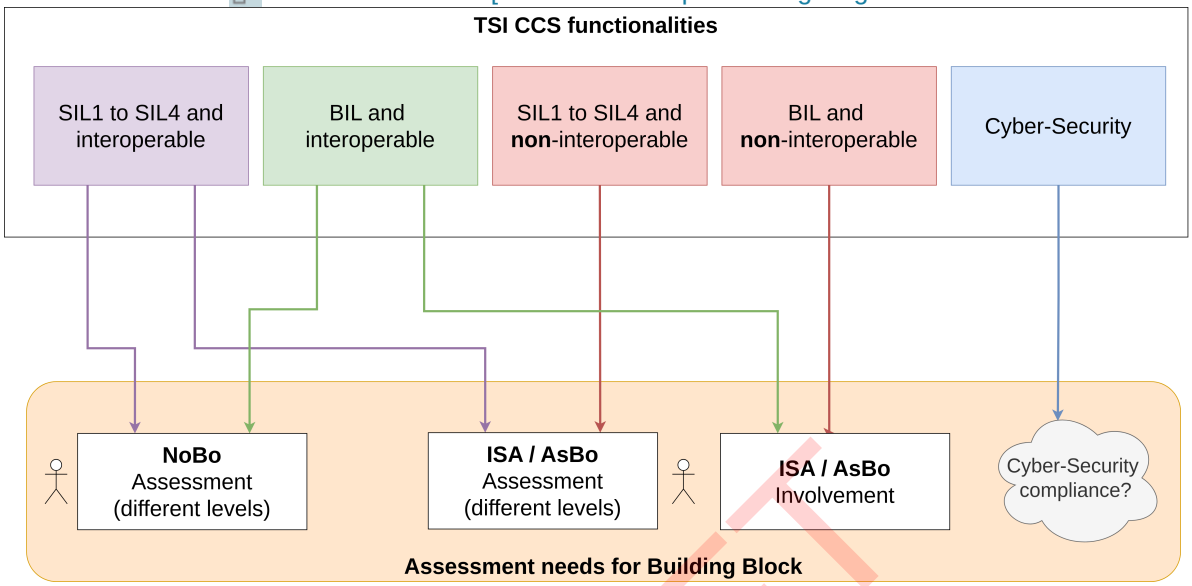


Figure 11 Separation rules within Building Block

[SPPRAMSS-16553, Rationale]

2.3.2 Change management in CSM-RA

Unified methodology in Europe for safety activities
In today's standard related to the interoperability world, SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] provides a unified methodology in Europe for managing safety activities in case of evolution of a railway system. CCS is basically covered by its scope in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] (refer to SPPRAMSS-8144 - Extract of Article 2 - Scope of CSM-RA and SPPRAMSS-8143 - Extract of 4.2.1.1. Safety in TSI CCS 2023).
[SPPRAMSS-1038, Text]

Extract of Article 2 - Scope of CSM-RA
3. This Regulation shall apply also to structural sub-systems to which Directive 2008/57 applies
=> today it is superseded by SPPRAMSS-4525 - [Directive 2016/797]

- (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
- 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.

[SPPRAMSS-8144, Text]

Extract of 4.2.1.1. Safety in TSI CCS 2023
(2) **other types of changes made by railway undertaking and infrastructure managers** (e.g. **changes** of the design or implementation of ETCS), as well as the **changes** made by other actors (e.g. manufacturers or other suppliers) **shall be managed according to the risk management process set**

out in Annex I to the Implementing Regulation (EU) No 402/2013, as referred to in Article 6(1)(a) of Directive (EU) 2016/798. **[**SPPRAMSS-8143, Text **]**

Proprietary methodology for risk assessment
The present document aims at providing a standardised way to handle evolution in CCS systems. However, it is foreseen in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] that proprietary methodology can be deployed to deal with risk assessment (refer to SPPRAMSS-8142 - Extract from CSM-RA [23]:ANNEX I). Therefore, the application of the present process should be mandatory only in case the user does not fulfil all safety requirements identified in the present process. In other case, the proprietary solution can still be applied on new projects. **[**SPPRAMSS-8145, Text **]**

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.

[SPPRAMSS-8142, Text **]**

2.3.3 Change management in CENELEC standards

Significance criteria
In addition to SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136], CENELEC standard SPPRAMSS-8147 - [EN17023: 2018] has also been analysed during this process realisation. Indeed, the latter uses the same criteria, with the same definition, as defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] but with more contextual data, processes and detailed examples of combination between the criteria reminded in SPPRAMSS-8148 - Annex A1 General - EN17023:2018. **[**SPPRAMSS-1039, Text **]**

Annex A1 General - EN17023:2018
This annex shows examples practiced in some countries to assess the significance of a maintenance plan modification. However, other methods can be applied. 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. **[**SPPRAMSS-8148, Text **]**

CSM-RA or EN50129 development process
Based on the previous statement, usually two different strategies are developed by the manufacturers:

- Apply the SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] and SPPRAMSS-8147 - [EN17023: 2018] 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 system or,
- Apply the CENELEC development process as allowed by SPPRAMSS-8142 - Extract from CSM-RA [23]:ANNEX I where the modifications management are presented in SPPRAMSS-8149 - Extract of section 1 Scope of EN 50129:2018.

[SPPRAMSS-1057, Text **]**

Extract of section 1 Scope of EN 50129:2018
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**.
[SPPRAMSS-8149, Text **]**

Additional systematic means for managing evolutions
Based on the last segment of SPPRAMSS-8149 - Extract of section 1 Scope of EN 50129:2018 “or supplemented by additional documentation”, the present document aims at proposing additional systematic means for managing evolutions without necessarily update the CCS systems or its constituent safety cases, depending on their criticality. This is the entry point for this evolution management process.
[SPPRAMSS-1072, Text **]**

2.4 ISA activities for evolved systems

Assessment activities
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.
[SPPRAMSS-1129, Text **]**

Management of evolutions during the CCS OB and its constituents’ lifetime
The management of evolutions during the CCS OB and its constituents’ lifetime is introduced by the CENELEC standards.
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****.* **[**SPPRAMSS-1130, Text **]**

Former EN 50506-2:2009
In addition, the former EN 50506-2:2009 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*

[SPPRAMSS-1136, Text **]**

Struggle
Today, there is a struggle when deploying this modifications process into SPPRAMSS-8880 - Generic Product Safety Case or SPPRAMSS-8881 - Generic Application Safety Case 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. **[**SPPRAMSS-1148, Text **]**

3 Modular Architecture

3.1 Concept of “ERTMS envelope”

Modular architecture evolution
Evolving a modular architecture comes with a lot of challenges related to configuration management, among else:

- evolution strategy concerning the individual architecture components when the specification of the overall system is changed (in our case: the relevant Sytem Pillar specifications and the TSI in particular), including the overall backward / forward compatibility strategy
- authorisation strategy when individual components of the architecture are changed (different version of the same product) or exchanged (replaced by a compatible other product)
- evolution and authorisation strategy for redundancy management in case of 'm out of n' redundant designs (in particular when not all of the instances may be changed in one 'big bang' go)
- management of changes in track topology, which is of particular importance if the changes in track topology are related to specification requirements implying conformity of the trackside infrastructure to different specification baselines / versions (maybe even with several phases where different track layout and field element integration are foreseen)

[SPPRAMSS-10239, Text **]**

Configuration envelope
If every conformity assessment, certificate and authorisation is always issued for one specific configuration and one specific environment of the system under consideration, and must be re-done if a change in one neighbouring component occurs, then the cost, effort and expectable time line of this are prohibitive. Therefore it is obvious that conformity assessments, certificates and authorisations must cover configuration variants as far as possible, considering:

- changes of the architecture component under consideration (as long as the intended functionality and interoperability is not changed substantially and no substantial new SRACs are to be respected -- e.g.: security updates) as well as
- changes in the environment of the architecture component under consideration (changes to interfaced components as long as a defined selection of interfaces / interface versions is met in specification and in dynamic behaviour of the overall system - in particular: which ETCS Baselines, national rules and additional functionalites are supported).

The set of compliant configurations covered by a certificate, assessment or authorisation should be and should be understood as a configuration envelope rather than a specific configuration.

This way, evolution of e.g. a vehicle to a newer ETCS Baseline is made possible by upgrading individual onboard components, operating in backward compatibility mode until all the necessary components are upgraded and the target baseline behaviour can be activated after only one final authorisation.
[SPPRAMSS-10190, Text **]**

Contribution of the safety management system(s) to the evolution of a modular architecture
Changes not explicitely causing a re-certification, re-assessment etc. are to be covered by safety assurance along two lines:

1. The safety management system established for the component under consideration for its post-deployment life cycle, including the generation of appropriate evidence along the necessary verification and validation activities
2. the safety management system and the interoperability management of the overall system, in particular in determining the necessary interoperability testing with other components of the overall system, including tracking the changes in the configuration management of the overall system.

[SPPRAMSS-10189, Text **]**

3.2 Concept of “safe integration”

"Safe integration" activities in the vehicle authorisation process
Several integration steps are required between the realization of a CCS-OB / TRK system until a train is authorized to run in operation on a dedicated network. The intermediates steps in between require the involvement of different actors and different equipment to be integrated with in many case safety requirements and application conditions.
As this integration steps do not only rely on ensuring the technical interoperability between them, ERA has provided a document which define a clear and complete frame for "safe integration" activities;
SPPRAMSS-9692 - [ERA 1209/063 V 1.0].

The picture below gives an example of where these "safe integration" steps occur today. They require a strong collaboration between the different stakeholders to be efficient.

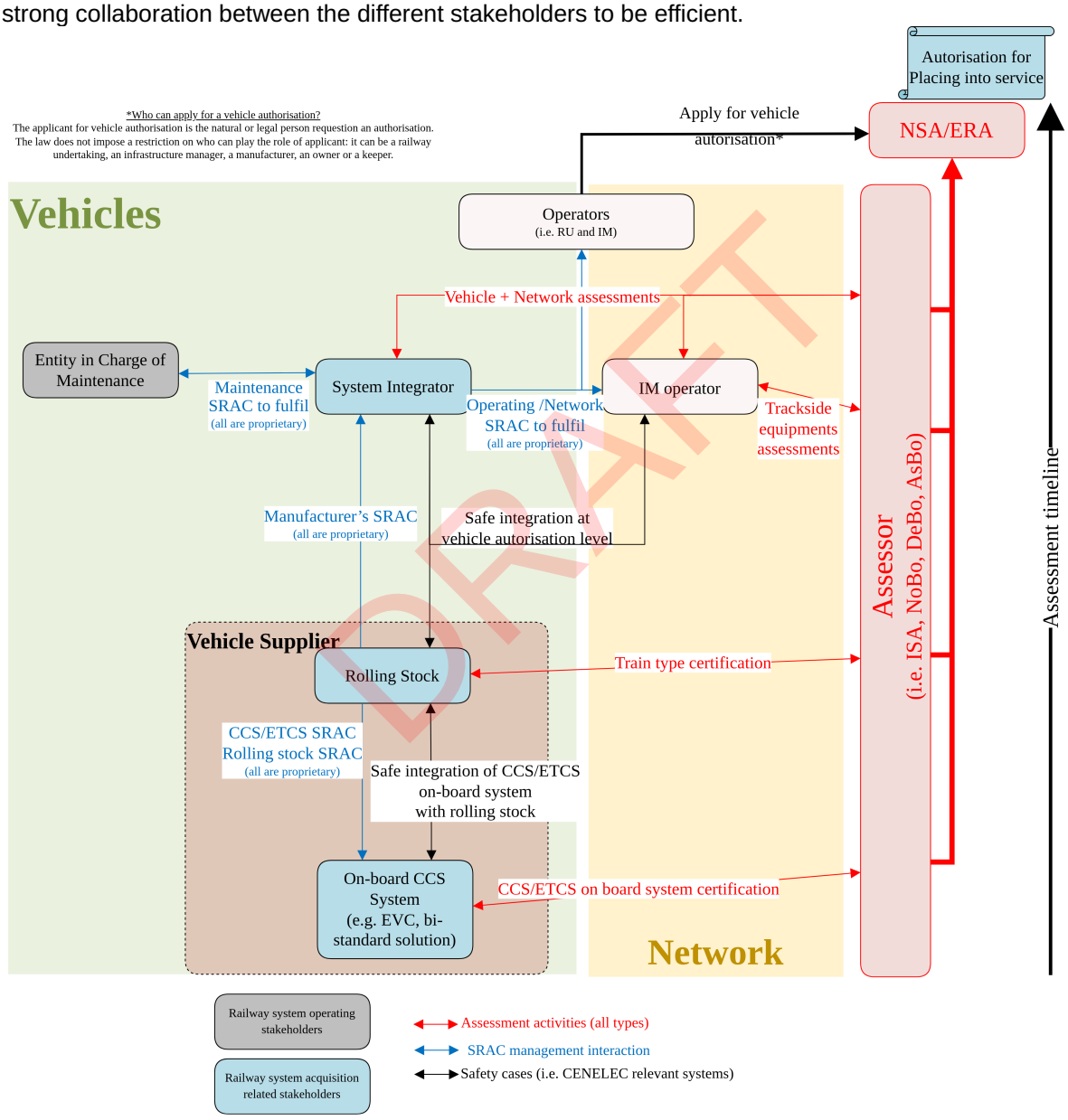


Figure 12 Example of current "safe integration" steps in authorisation process

[SPPRAMSS-1096, Text]

"Safe integration" in a modular architecture
One major goal of System Pillar is to define a modular architecture of the CCS system (i.e. on-board and

trackside). This means that more stakeholders will be involved from the CCS system certification until the final authorisation for placing into service of a couple train+network. Indeed, the "safe integration" will start at the building of the CCS system based on modular building blocks.
In addition to the modular CCS systems, the standardization of the CCS-Rolling stock interface (i.e. through SPT2TRAIN-2269 - Subset-119 - Train Interface FFFIS, Version 4.0.0) may bring another step of "safe integration". Indeed, in the future, a CCS-OB retrofit could be done without the original supplier of the rolling stock.

Knowing that, the figure below intends to present a possible future ERTMS project approval frame that integrates ERJU SP requirements for a modular architecture. It must be noticed here that the actors name here are not yet standardized and are presented here only to show the additional steps and stakeholders induced by bringing modularity.

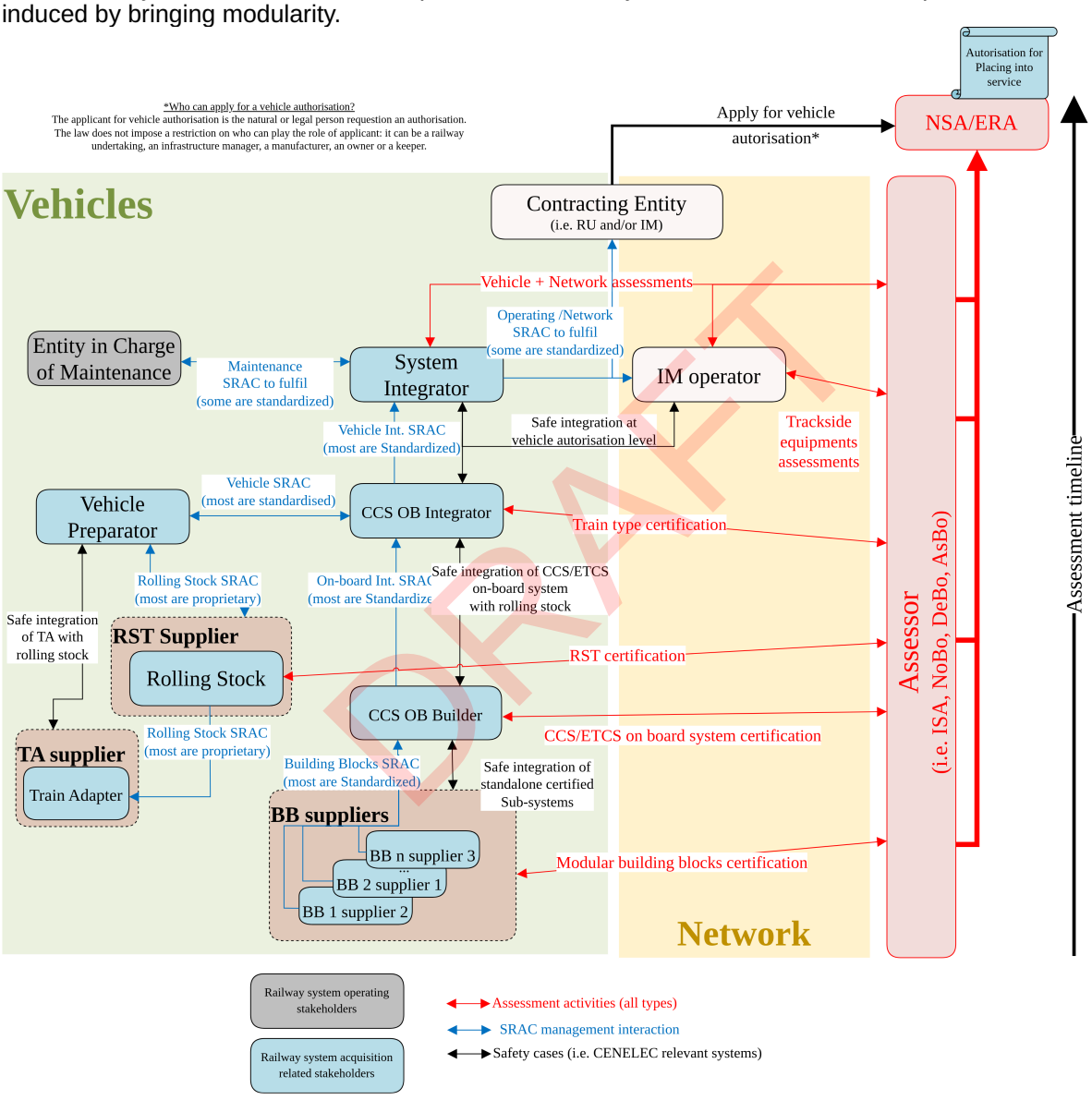


Figure 13 Example of future "safe integration" process in a modular architecture

With comparison between the past and new frames of authorisation, it can easily be deducted that the new process may be much more complex and long that the original one because of all new stakeholders dealing with "safe integration" activities. **[**SPPRAMSS-1099, Text **]**

Safe integration in Commission Implementing Regulation 2018/545
SPPRAMSS-327 - [Commission Implementing Regulation (EU) 2018/545 + (EU) 2020/781] warns the

different stakeholders about misunderstandings regarding the concept 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. **[**SPPRAMSS-1105, Text **]**

Requirements of ERA clarification note on safe integration

Following that, SPPRAMSS-9692 - [ERA 1209/063 V 1.0] 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.*

[SPPRAMSS-1119, Text **]**

Authorisation process in a modular architecture

The PRAMS and SP teams involved in the definition of a future process (i.e. TrainCS and TrafficCS) from CCS system to authorisation for placing into service shall define a process to allowing to exploit the benefits of a modular architecture without undergoing or underestimating its complexity.
To reach that, the concept of "safe integration" defined in SPPRAMSS-9692 - [ERA 1209/063 V 1.0] recapped in SPPRAMSS-1119 - Requirements of ERA clarification note on safe integration shall be fully addressed:

- Definition of standardised list of stakeholders
- Define for each of them role, tasks, responsibilities and interactions:
  - Input(s) expected to realise the activities (from previous level of system integration),
  - Output(s) expected (to next level of system integration),
- Define an assessment/authorisation frame clear for each level (new or adapted from existing) from building block to Authorisation for placing into service.

[SPPRAMSS-9694, Text **]**

No definition of integration activities

The first version of the document is not completely covering the management of evolutions at CCS integrated system level.
The main focus of SC2.3 and SC2.4 is the management of evolutions at building block level.

The ideas from the OCORA Approval process should be analysed in a future version of this document..

This should have a 2 dimension view:
- Safe integration of evolving building blocks
- Make sure safe integration is still possible with an evolving reference architecture

The Innovation Pillar - FP2 R2DATO - WP26 is analysing the state of the authorisation process and its compatibility with a modular architecture. The conclusions of its deliverable D26.4 "Summary of findings and recommendations from study on modular certification and homologation" shall be taken into account in a next version of this document.
[SPPRAMSS-10153, Issue, Open, Bois Julien (I-NAT-GST-CCS-EXT - Extern) **]**

3.3 Computing Environment - Prerequisites for evolutions

3.3.1 Introduction to the Computing Environnement

Introduction

The modularity of a system is directly influenced by the computing environment. Modularity can be realized at different layers of the system solution. Therefore, the computing platform plays a crucial role in ensuring module creation, independence or mutual communication, availability, safety and security and other properties. Depending on the approach, achieving modularity may involve leveraging platform features, which may simplify implementation of applications with protecting the system properties. However, this may also increases cost due to the complexity of platform changes and certification requirements.
Modularity can be achieved through separate hardware components without relying on platform features, or it can be addressed at the application layer. Evaluating the effectiveness and selecting the appropriate approach is beyond the scope of this document and PRAMS group within SP. Instead, this document

summarizes different options with effect on safety or security assessments within evolution management. **[**SPPRAMSS-8240, Text **]**

Safety and Security Building Blocks for the Modular Architecture
The technologies used for the modular platform are well known also in different engineering areas. The building blocks synergies and trade-offs in sense of safety and security have been analyzed in document D2.1 in the SPPRAMSS-9986 - SESAMO Project
[SPPRAMSS-8901, Text **]**

Computing Environnement
The Computing Environment is defined in System Analysis , which describes the different modules and contains the following logical architecture. **[**SPPRAMSS-15974, Text **]**

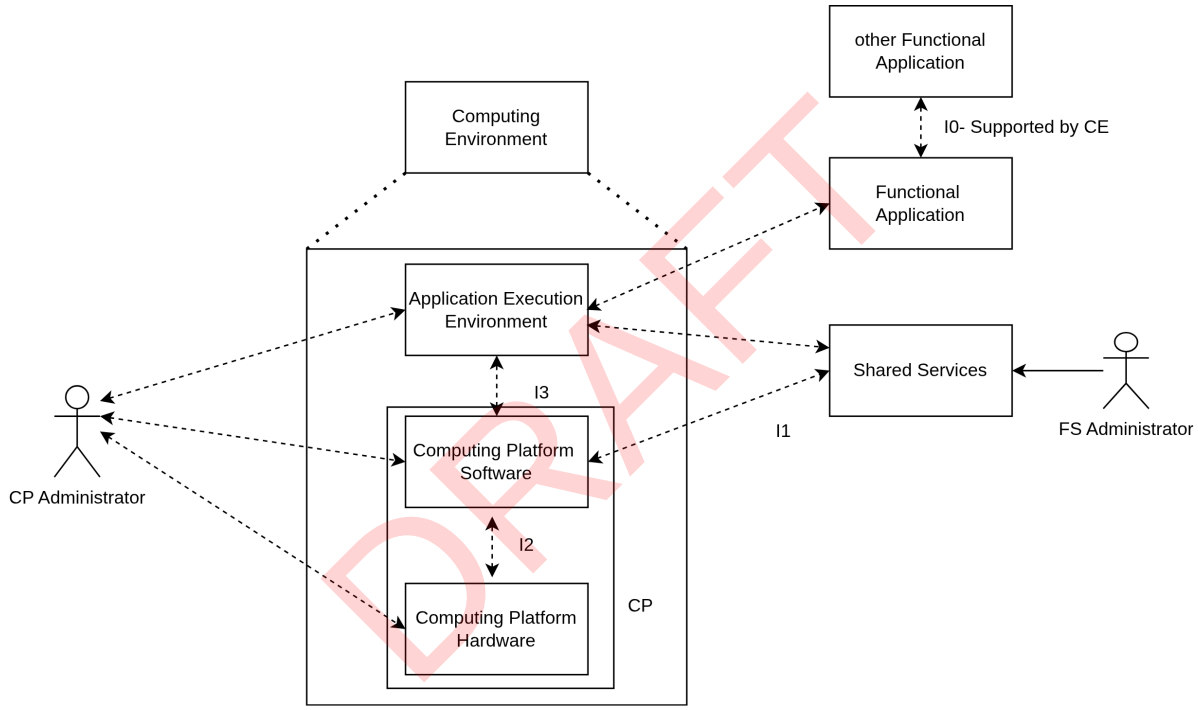


Figure 1 CEnv Logical Architecture

Subsystems:

- **SPT2CE-1239 - Application Execution Environment**
- **SPT2CE-2443 - Computing Platform Software**
- **SPT2CE-2442 - Computing Platform Hardware**

External Actors/Systems:

- **Functional Application**: Railway application deployed on the AEE.
- **Shared Service**: Common services (e.g., Configuration, update, diagnostic, security).
- **CP Administrator**: manages Computing Platform
- **FS Administrator**: Manages Functional System

Interfaces:

- **I0**: Connects railway functions running on CEnv with other railway functions (running on CEnv or external platforms).
- **I1**: Connects external systems (Shared Service, Administrator) to the CEnv.
- **I3**: Connects the AEE to the CPSW.
- **I2**: Links the CPSW to the CPHW.

3.3.2 PRAM requirements for the Computing Environment

PRAM requirements for the Computing Environment
PRAM requirements for the Computing Environment are defined in PRAMS Requirements.
[SPPRAMSS-15647, Text **]**

3.3.3 Long term maintenance strategy and modularity for the Computing Environment

Second sourcing of building blocks
It shall be possible to replace the COTS Computing Platform hardware by at least two references of Computing Platform hardware, coming from at least two different suppliers.

ID	SPPRAMSS-13876
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Evolvability of the Computing Platform
It shall be possible to update the Computing Platform Software without impacting the virtual building block running on it.

ID	SPPRAMSS-13884
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Evolvability of non-application software
It shall be possible to update the non-application software (e.g. OS, communication layer with Computing Platform) of a virtual building block without impacting the functions (i.e. the application itself).

ID	SPPRAMSS-13883
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Virtual Building Blocks Suppliers
It shall be possible to replace a virtual building blocks from Supplier A, by an equivalent virtual building block from Supplier B.

ID	SPPRAMSS-13888

To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Decoupling of the Software and Hardware Architecture
The computing platform software shall be designed to run any guest OS within the virtualised environment of the Virtual Building Blocks, independent of the underlying hardware architecture, including CPU architecture.

For example, the system shall support running guest OSs (e.g., x86 or ARM-based) on different processor architectures, enabling seamless hardware upgrades over the lifetime of the system.

ID	SPPRAMSS-14274
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

3.3.4 Safety requirements for the Computing Environment

Non-interference between virtual building blocks
The non-interferences between two virtual building blocks running on the same hardware shall be demonstrated.

ID	SPPRAMSS-13877
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Non-interference between building blocks and the Computing Platform
The non-interference between virtual building blocks and the Computing Platform Software shall be demonstrated.

ID	SPPRAMSS-13875
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

BIL Function on a single hardware
It shall be possible to run on the Computing Platform Software a BIL function on a single COTS hardware.

ID	SPPRAMSS-13881
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

SIL / SIL2 Function on a single hardware
It shall be possible to run on the Computing Environment a SIL1 / SIL2 function on a single COTS hardware (certified according to the required SIL from SPPRAMSS-334 - [EN 50129:2018/AC:2019-04]).

ID	SPPRAMSS-13880

To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Types of failures
The Computing Environment solution shall fulfil the SIL and TFFR requirements allocated by the System Pillar domains despite the architecture used to implement the railways functions (i.e. Computing Platform Software + virtual building block(s) + Hardware Commercial Off-the-Shelf). The following failure modes are considered:

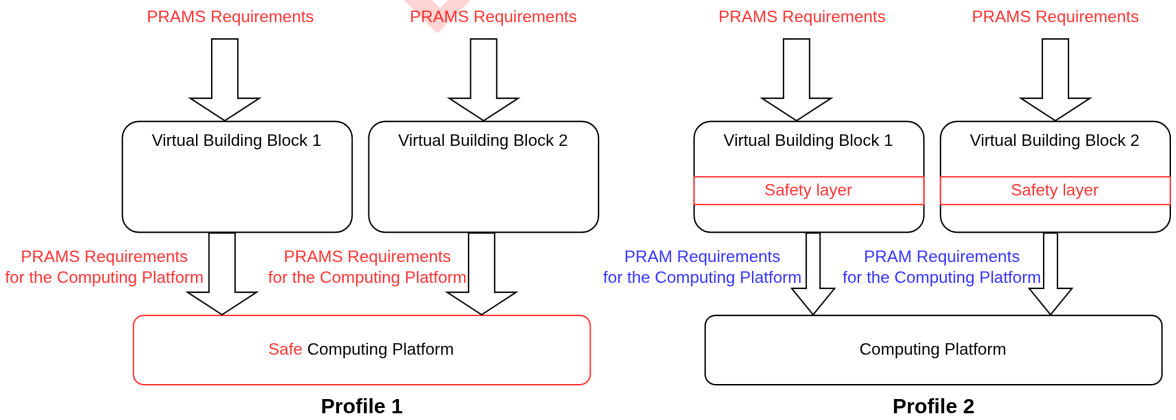
- No Function / data / message
- Deletion of function / data / message
- Untimely (i.e. wrong moment, too soon, too late, too quick, too long) function / data / message
- Corruption function / data / message
- Freeze of function / data / message
- Repetition of function / data / message
- Insertion of data / message
- Re-sequencing of data / message
- Masquerade (i.e. security threat) of function / data / message
- Partial of function / data / message

Note: a particular attention is expected with the use of non-safe Computing Platform Software + Hardware Commercial Off-the-Shelf with SIL1 to SIL4 virtual building blocks.

ID	SPPRAMSS-13882
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Computing Platform Software - EN50716
The Computing Platform Software (e.g. OS + hypervisor + hardware ressources access) shall respect the PRAM(S) requirements assigned by the SP Domains. In particular either by:

- having the Computing Platform Software developed according to the EN50716 or
- imposing the use of a safety-layer implementing the EN50716 requirements inside its virtual building block(s).



ID	SPPRAMSS-14404
To be derived by Team	SP Task 2 CONEMP Computing Environment

Type	System Requirement

Computing Environment Strategies
The PRAMS requirements of virtual building block(s) toward the Computing Platform Software are harominsed by the SP Domains (e.g. Train CS, Traffic CS). These requirements will be made available in different architecture profiles. There are 2 main potential profiles:

- Profile 1 : Certified Computing Platform Software according to EN50716; this profile is not yet considered by the SP Computing Environment and might be more adapted to on-board use cases,
- Profile 2 : COTS Computing Platform Software (not certified according to EN50716) and a Safety layer within the virtual building blocks (developped according to EN50716); this profile is considered by the SP Computing Environment and might be more adapted to trackside use case.

[SPPRAMSS-14420, Rationale **]**

Computing Platform Software - Pre-existing software
If the Computing Platform Software is using non-railways COTS software, the EN50716 requirements concerning pre-existing software shall be fulfilled (refer to SPPRAMSS-13909 - Re-use of widely deployed COTS).

ID	SPPRAMSS-13889
To be derived by Team	SP Task 2 CONEMP Computing Environment
Type	System Requirement

Consideration of other PRAMS requirements
Requirements in the chapter above are related to the evolution management process. To ensure the smooth execution of the process, it is necessary to consider also other PRAMS requirements specific to the computing platform listed in PRAMS Requirements **[**SPPRAMSS-15655, Text **]**

3.3.5 Security requirements for the Computing Platform

IEC CDV 63452 - Railway applications – Cybersecurity
The new standard IEC CDV 63452 "Railway applications – Cybersecurity" shall be analysed for the next version of this document.
The EU Rail System Pillar Cybersecurity Specifications version 1.09 shall be analysed for the next version of this document.
[SPPRAMSS-15347, Issue, Open, SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) **]**

3.4 Cyber-Security - Prerequisites for evolutions

3.4.1 Introduction, scope and goal

Introduction to Cyber-security evolutions
In the near future it is likely that cyber-security attacks on safety-related systems on-board of rolling stock and on trackside systems will be more common than nowadays for several reasons:

- more connectivity of the systems,
- use of open and common communication protocols,
- hybrid warfare by enemy countries,
- exploitation of system vulnerabilities (e.g. malware, fishing)

To face these 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 cyber-attack by correcting cybersecurity issues or implementing new cyber-security measures in a much much shorter time than what is normally done on safety-related systems.

Such process is not defined in the SPPRAMSS-8814 - [EN 50716:2023]. This standard only states "It may be necessary to balance between measures against systematic errors and measures against security threats. An example is the need for fast security updates of software arising from security threats, whereas if such software is safety related, it should be thoroughly developed, tested, validated and approved before any update." **[**SPPRAMSS-8837, Text **]**

Cyber-security zoning
Cyber-security zoning (refer to SPPRAMSS-5833 - IEC 62443 2-1, 2-4, 3-2, 3-3, 4-1, and 4-2) involves segmenting the network into distinct zones based on system criticality and sensitivity. Each zone implements tailored security controls, like firewalls, access controls, IDPS, and data encryption, to manage and mitigate risks. Continuous monitoring, incident response plans, and regular audits ensure effective threat detection and response. This approach helps prevent a breach in one zone from affecting others, ensuring safe and efficient railway operations.

This is reflected in Secure Component Specification. **[**SPPRAMSS-8839, Text **]**

Necessity of having a fast process
A fast process for the security evolution (developing, testing, homologation and roll-out is needed (see SPPRAMSS-15256 - Shortcuts to the Significance Process).

In some cases, a security issue could have a high RAMS impact, and it might be complicated to implement mitigation measures. In this case, it might be urgent to update the software.

In case of a cyber-security issue, several criteria are analysed.
For example :

- Exposure and emerging vulnerabilities: is the code exposed or not ? is it a determined attack ? Is it a blind attack by a random virus ?
- Consequences : does it have Safety or Availability consequences ? Does it impact 1 train, several trains, a complete fleet, ...) ?
- Mitigation measure : is it necessary to stop the train or the fleet to avoid the risk ?

However, with the current systems in operation, often enough mitigation measures can be taken and there is no urgency to update the software. **[**SPPRAMSS-9887, Text **]**

3.4.2 Architecture

Possible architecture of the security services within the computing platform
The architecture of the shared security services within the Computing Platform Environnement is not defined yet.
The following drawing is just for illustration.

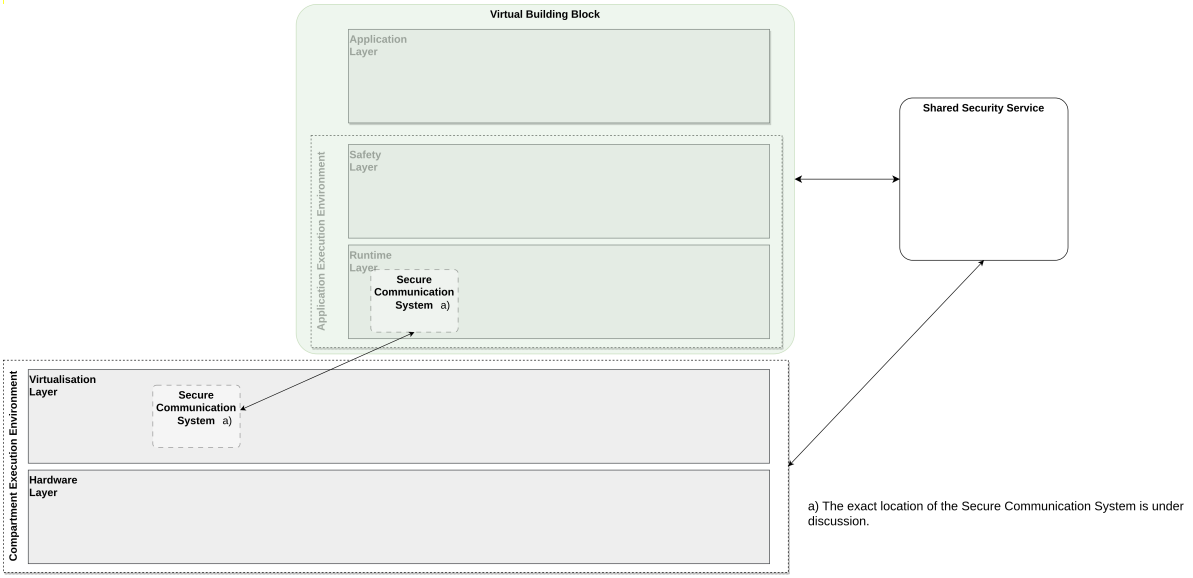


Figure 14 Possible Architecture for the Shared Security Services within the Computing Environnement

[SPPRAMSS-14402, Text **]**

3.4.3 Security Requirements

EN50716 / EN50129 and Cyber-security
The railway standards SPPRAMSS-8814 - [EN 50716:2023] and SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] mention cyber-security in safety-related systems.

- The SPPRAMSS-8814 - [EN 50716:2023] does not cover cyber-security activities inside a safety-related software (see Introduction of the standard)
- The SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] provides two requirements that cover cyber-security on a safety-related system (see the chapter 6.4 of the standard)

[SPPRAMSS-15349, Text **]**

Cyber-Security functionalities
To avoid using the SPPRAMSS-8173 - Evolution Management process as much as possible for cyber-security-related updates, most of the cyber-security functionalities shall be outside the safety-related software, and implemented in the SPPRAMSS-14403 - Shared Security Services - IEC 62443-2-3.

ID	SPPRAMSS-14907
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Cyber-Security and evolutions of a safety-related software
If it is necessary to update a safety-related software for cyber-security reasons, the SPPRAMSS-8173 - Evolution Management process shall be applied.

ID	SPPRAMSS-14908
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP

Type	System Requirement

Scope of the present document concerning Cyber-security evolutions
In case of a cyber-security-related evolution is needed, the RAMS impact shall be analysed.

ID	SPPRAMSS-9888
To be derived by Team	SP Task 2 Train CS, SP Task 2 TrafficCS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Shared Security Services - IEC 62443-2-3
The Shared Cybersecurity Services shall be developed according to the IEC 62443-2-3 : "The development shall be formalised in a patch/update policy of the organisation", to allow frequent and fast evolutions.

ID	SPPRAMSS-14403
To be derived by Team	SP Task 2 Train CS, SP Task 2 TrafficCS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Shared Security Services - Non-interference with virtual building block software
The Shared Cybersecurity Services shall be designed to ensure non-interference with any virtual building block software, to allow frequent and fast evolutions.

ID	SPPRAMSS-14406
To be derived by Team	SP Task 2 Trackside Asset CS, SP Task 2 Train CS, SP Task 2 TrafficCS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Non-interference between Shared Security Services and software developped according to EN 50716
The virtual building block (functional systems) are developed according to the EN 50716 as requested in SPPRAMSS-13905 - Software development process for initial release.

Compliance with the SPPRAMSS-14406 - Shared Security Services - Non-interference with virtual building block software shall be demonstrated to allow the Shared Security Services to be developed according to the applicable cyber-security standard (covered by the cyber-security requirements), instead of the EN 50716.
[SPPRAMSS-16554, Rationale **]**

Use of Shared Security Services
Shared Security Services, as proposed by the Cybersecurity Domain and reference architecture, are intended to support—not replace—the cyber-security protection efforts of safety-related railway functions. When implemented with appropriate isolation, hardening, and monitoring, shared services can contribute to risk management by:

- Reducing complexity within safety-related applications, which in turn minimises the potential for integration errors and unintended interactions,
- Limiting the scope of changes required in safety-qualified software, by handling evolving cyber-security threats externally to the safety logic,
- Supporting the update of the most vulnerables devices (e.g. fleet updates).

[SPPRAMSS-9889, Rationale **]**

Evolution of a virtual building block for cyber-security reasons
The evolution of a virtual building block for cyber-security reasons outside the Shared Cybersecurity Services shall be developed according to the EN50716 (e.g. : patch in the application layer, the safety layer or the runtime layer within the functional system).

ID	SPPRAMSS-14405
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Trackside Asset CS, SP Task 2 Train CS, SP Task 2 CONEMP, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Non interference of the software components implementing the Secure Component Specification
The cyber-security-related software components (as defined in EN50716 §3.1.4) of a secure component implementing the software requirements of the Secure Component Specification shall be designed to ensure non-interference with the safety-related software components.
This is linked with the SPPRAMSS-2503 - The Secure Component shall ensure that the safety functionality is not influence...

ID	SPPRAMSS-14410
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Cyber-security and Significance
If the requirements SPPRAMSS-14406 - Shared Security Services - Non-interference with virtual building block software and SPPRAMSS-14410 - Non interference of the software components implementing the Secure Component Specification are respected, the cyber-security process can be used to develop, test and assess the evolution of the Shared Cybersecurity Services. The SPPRAMSS-5682 - Update and configuration management still applies, to ensure general compatibility with the System Pillar architecture.

If a cyber-security-related evolution is impacting / interfering with a safety-related function or component:

- the SPPRAMSS-1167 - Significance process shall be used,
- the Common Vulnerability Score (CVSS - see https://www.first.org/cvss/v4-0/specification-document) can be used to evaluate the SPPRAMSS-8815 - Urgency Criteria of the evolution.

ID	SPPRAMSS-15348
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Integrity and authenticity of software
Transversal CCS shall respect the requirement SPPRAMSS-12229 - The railway shall define a procedure to check the integrity and authenticity of... .

ID	SPPRAMSS-14409
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Process for test and installation
The WG Transversal CCS shall respect the requirement SPPRAMSS-12231 - The railway shall implement a process to check software before test and installa...

ID	SPPRAMSS-14407
To be derived by Team	SP Task 2 Train CS, SP Task 2 TrafficCS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

Firmware of Secure Components
No safety-related functions shall be allocated to the firmware of Secure Components.

ID	SPPRAMSS-14411
To be derived by Team	SP Task 2 Train CS, SP Task 2 TrafficCS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment, SP Task 2 CONEMP
Type	System Requirement

3.5 FFF Interfaces - Prerequisites for evolutions

FFF Interfaces for onboard applications
System Requirements defining standardised electric (e.g. voltage power supply) and mechanical interfaces (e.g. connectors, rack, cabinet size), environmental (e.g. heat, vibration, humidity) shall be defined by the WG TrainCS to allow evolutions within a modular architecture.

ID	SPPRAMSS-14690
To be derived by Team	SP Task 2 Train CS
Type	System Requirement

FFF Interfaces for Trackside Assets applications
System Requirements defining standardised electric (e.g. voltage power supply) and mechanical interfaces (e.g. connectors, rack, cabinet size), environmental (e.g. heat, vibration, humidity) shall be defined by the WG Trackside Assets to allow evolutions within a modular architecture.

ID	SPPRAMSS-14691
To be derived by Team	SP Task 2 Trackside Asset CS
Type	System Requirement

FFF Interfaces for Traffic CS applications
System Requirements defining standardised electric (e.g. voltage power supply) and mechanical interfaces (e.g. connectors, rack, cabinet size), environmental (e.g. heat, vibration, humidity) shall be defined by the WG Traffic CS to allow evolutions within a modular architecture.

ID	SPPRAMSS-15662
To be derived by Team	SP Task 2 TrafficCS
Type	System Requirement

4 Evolution Management process

4.1 Impact and objectives of the evolution management process

Impact and objectives of the evolution management process
The Evolution Management Process is a crucial component within the railway sector, aimed at overseeing upgrades and updates to railway subsystems throughout their operational phase.

This process is a key part of ensuring that changes maintain appropriate standards of safety and efficiency.

Evolution management is designed to support railway operators and suppliers in navigating these challenges by offering a structured approach to enhancing existing systems. Its role is to safeguard safety standards, ensure compliance, and facilitate improvements without disrupting operations.

Within the System Pillar, evolution management is vital, as it underpins the continuous, safe improvement of the railway system, ensuring it meets the evolving demands of modern rail transport.

This system requirement is the "head system requirement" of this document :

- linked to the relevant System Pillar Common Business Objectives
- linked to the other system requirements from this document

The traceability is available in this annex: Evolution Management Traceability

ID	SPPRAMSS-11459
Type	System Requirement

Traceability between Common Business Objectives and System Requirements
The traceability between Common Business Objectives and the System Requirements from this document is visible in the :
Evolution Management Traceability, but not visually in the document.

An official annex should be created, for the .pdf export.

The text of the SPPRAMSS-11459 - Impact and objectives of the evolution management process should also be updated.
[SPPRAMSS-10240, Issue, Open, SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) **]**

4.2 Methodology deployed to develop evolution management

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

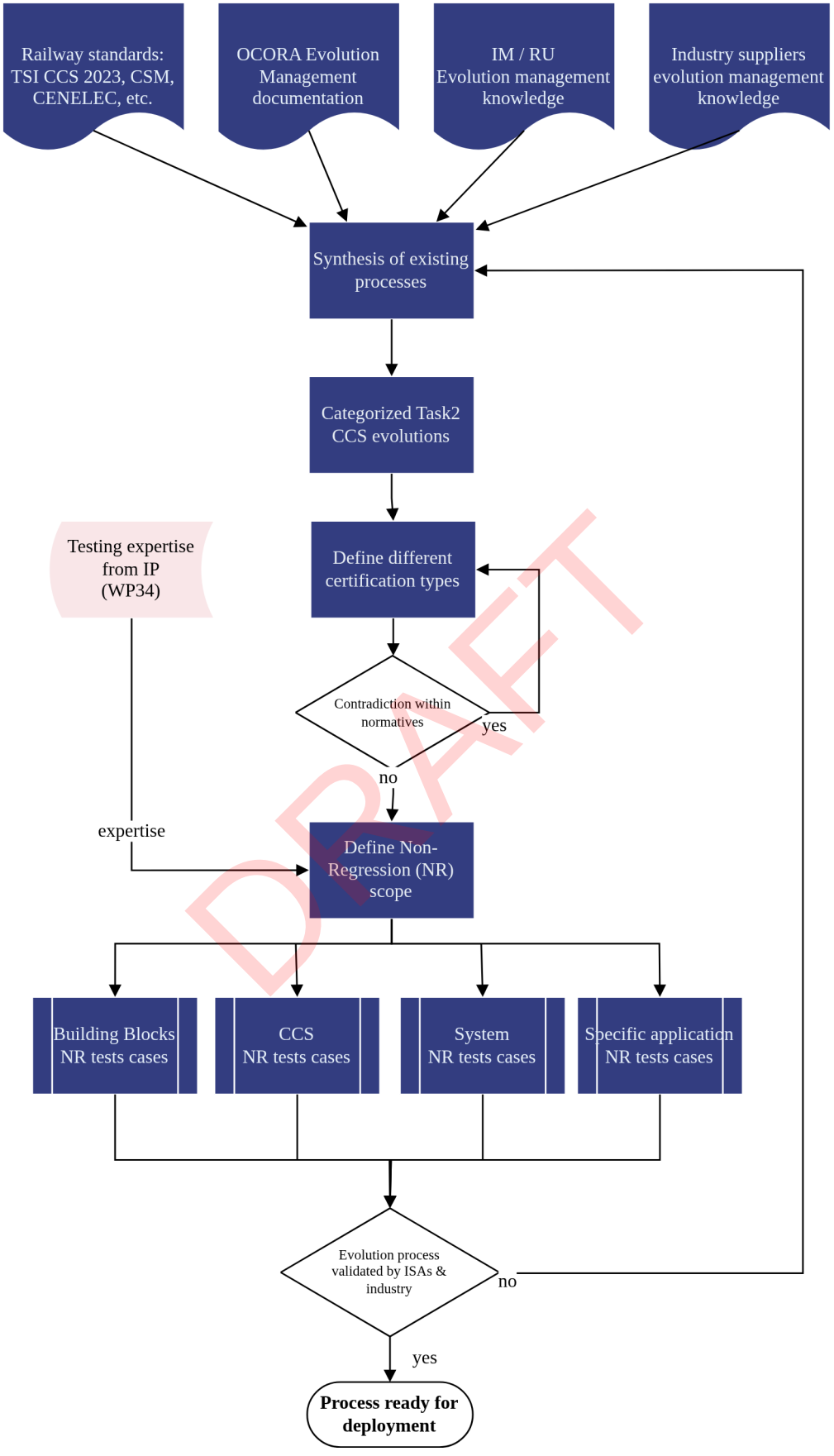


Figure 15 Evolution process methodology

[SPPRAMSS-5668, Text]

This methodology is based around 4 main steps:
This methodology is based around 4 main steps:

1. *Synthesis of existing processes*: research of existing railway documentation applicable when dealing with evolutions:
    - Railway documentation under consideration as for example TSI CCS 2023, CSM-RA, CENELEC, etc.
    - OCORA evolution management documentation: evolution management process focused on CCS-OB.
    - IM / RU evolution management knowledge: common practices from IM's and RU's point of view related to evolution management of their projects.
    - Industry suppliers evolution management knowledge; common practices from Industry suppliers for evolution management of their generic products, generic applications, specific applications, etc.

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

2. *Categorized Taks2 CCS evolutions* : the second step consists in defining which type of evolutions in the Task2 CCS system are covered by the process.
3. *Define different certification types*: one key activity of this process is to propose different shades of assessments based on the evolution impact. This evolution impact is categorized through a Significance evaluation process.
4. *Define Non-Regression (NR) tests scope*: to define a typical scope of non-regression tests for each type of classified evolutions:
    - For each building block or type of building blocks.
    - For the CCS integrating the evolved building block(s),
    - For the System integrating the CCS subsystem with other susbsystems.
    - For the specific application.

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. assessment body) for review. [SPPRAMSS-1033, Text]

Application of software metrics
Important means to perform the steps defined in SPPRAMSS-1033 - This methodology is based around 4 main steps: is gathering relevant information about software affected by the changes.
Software metrics offer a standardised, effective, well defined and structured view on software. Therefore, these steps should always be performed using software metrics adequate to the intended changes and the affected software.
Standard SPPRAMSS-8814 - [EN 50716:2023] and the present process discuss a selection of metrics to determine software complexity as a starting point (refer to SPPRAMSS-13903 - Software Complexity Metrics). [SPPRAMSS-13911, Text]

4.3 Overview of the Evolution Management Process

Overview of the Evolution Management process
The Evolution Management 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 building block requirements, bug fixing) or the users (vehicle owner or infrastructure manager) requires a change in the CCS constitution (e.g. new BB, change of supplier for a BB)
- 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 system pillar scope);

- use of significance matrix: this tool, defined by the WG PRAMS aims at determining the relevant level of assessment required based on the technical impact analysis.
- result of the significance process comes from:
  - complete analysis of the significance critieria defined in SPPRAMSS-8169 - Combination of criteria in the Significance Matrix or,
  - "shortcut" processes defined in SPPRAMSS-15256 - Shortcuts to the Significance Process
- consolidation of the process requirements: this steps considers both:
  - Significance critieria defined in SPPRAMSS-8174 - Significance Criteria and,
  - TSI CCS conformity criteria defined in SPPRAMSS-15267 - TSI CCS conformity process
- Sw and Hw development: these activities, performed by the user with its own process, represents the implementation of the evolution,
- testing the evolution:
  - determine tests impact (to be defined in a future version): 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 CCS 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. The development of testing activities related to the Evolution Management Process will start during remit 2024-2025 as explained in SPPRAMSS-9693 - Connection between PRAMS and IP FP2 R2DATO WP34/35 Testing .
  - represents the execution of the tests at different levels (if relevant) determined during the tests impact phase,
- homologation reports of the evolution: this activity, performed by the user with its own process, represents the homologation of the evolution with an assessor

A flowchart of the process is available in the following annex SPPRAMSS-15981 - Annex - Flowchart of the Evolution Management Process **[**SPPRAMSS-15673, Text **]**

4.4 Significance process

4.4.1 Introduction to the Significance process

Introduction Significance process
To determine the significance of an evolution, the following Significance process is defined.
Several criteria are analysed, combined in a Significance matrix and then used as an input for:

- the Software Development process
- the Hardware Development process
- the Testing process
- the Homologation process

[SPPRAMSS-1238, Text **]**

Error correction in the source code
In case of an error correction of the source code deviating from intended functions and/or performance, as described in SPPRAMSS-14396 - Error correction, the significance process is simplified: only the requirement SPPRAMSS-14398 - Level of Significance of an error correction in the source code applies. **[**SPPRAMSS-14397, Text **]**

Impact analysis
Before applying the Significance process, an Impact analysis of the evolution shall be carried on by a team composed of at least the Safety Manager, the Requirements Manager, the Designer and the Implementer (roles defined in the CENELEC standards).

The impact analysis shall be include:

- a description of the content of the evolution and its goals
- a list of impacted and modified functions
- a list of impacted and modified hardware / software
- a list of impacted interfaces

ID	SPPRAMSS-1170
Type	System Requirement

4.4.2 Significance Criteria

Introduction to Significance Criteria
In this chapter, seven Significance criteria are defined to analyse an evolution.

Each criterion is evaluated to one of the values MINIMAL / LOW / MIDDLE / HIGH.

For each of the values MINIMAL / LOW / MIDDLE / HIGH, points are assigned.

The criteria suggests how the evolution should be developed, tested and homologated.
[SPPRAMSS-8817, Text **]**

4.4.2.1 Additionality

Additionality in case of evolution
The Additionality criteria is defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] 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.

The additionality consists in analysing the gap between the last valid ISA certificate and the current situation.

This means checking the complexity and of previous evolutions made on the SuC and number of Change Requests implemented since the last ISA certificate.

The additionality shall be analysed, by calculating :

- the sum of the SPPRAMSS-1241 - Complexity scores of all the previous evolutions on the SuC since the last ISA certificate,
- the sum of the SPPRAMSS-14903 - Change Requests implemented on the SuC since the last certificate.

Table 5 Management of Additionality criterion

Additionality	MINIMAL (1)	LOW (2)	MIDDLE (3)	HIGH (4)
Sum of the SPPRAMSS-1241 - Complexity scores of all the previous evolutions on the SuC since the last ISA certificate	Sum < 5	5 <= Sum < 10	10 <= Sum < 15	Sum >= 15
Sum of the SPPRAMSS-14903 - Change Requests implemented on the SuC since the last ISA certificate	Sum < 50	50 <= Sum < 100	100 <= Sum < 150	Sum >= 150

ID	SPPRAMSS-1173
Type	System Requirement

Additionality in case of error correction
The supported acceptable residual error rate shall be defined by the ISA/AsBo assigned to the Building Block assessment.

Note : The context and and conditions are presented in :

- SPPRAMSS-15259 - Rationale on Additionality in case of error correction
- SPPRAMSS-15264 - Rationale for Yearly Letter of Support (yLoS)

ID	SPPRAMSS-15260
Type	System Requirement

4.4.2.2 Failure consequence

Failure consequence
The Failure consequence criterion is defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] as follow:
(a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment [see SPPRAMSS-1001 - Limitation of scope for the first and second version], *taking into account the existence of safety barriers outside the system;*

The failure consequence of the functions impacted by the evolution shall be analysed.

Table 6 Management of Failure Consequence criterion

Failure consequence	MINIMAL (1)	LOW (2)	MIDDLE (3)	HIGH (4)
What is the safety integrity level of the functions impacted by the evolution ?	BIL (no safety related functions impacted)	BIL (one or several safety-related BIL functions impacted)	SIL1 or SIL2 functions impacted	SIL3 or SIL4 functions impacted

ID	SPPRAMSS-1234

Type	System Requirement

4.4.2.3 Innovation/novelty

Innovation/novelty
The Innovation/novelty criterion is defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] 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;

As a basis forthe criterion, the definitions from the Swiss national regulation RTE 49100 are re-used and adapted to the CCS.

The innovation/novelty of the evolution shall be analysed, by answering the following questions:

1. Can a technical code of practice (e.g. norms, directives) be used to develop the evolution ?
2. Had the evolution already been successfully deployed on similar products/system in commercial revenue without any critical failure of the evolution detected so far?
   Note: competitors have similar products already on the market
3. Does the evolution remain in the actual state of technique (e.g. FRMCS, ATO GoA 3/4 are beyond actual scope)?
4. Does the evolution correspond to the reference system defined by TSI CCS 2023?

Table 7 Management of Innovation criterion

Innovation	MINIMAL (1)	LOW (2)	MIDDLE (3)	HIGH (4)
Number of answers "NO" to the questions	0 answers	1 answer	2 answers	3 or 4 answers

ID	SPPRAMSS-1235
Type	System Requirement

4.4.2.4 Complexity

Complexity
The Complexity criterion is not properly defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] and is ambiguous.

The following list of technical items is proposed to define the complexity of an evolution. It is not exhaustive and should be considered as as informative:

The Complexity of the evolution shall be analysed.

Table 8 Management of Complexity criterion

Complexity	MINIMAL (1)	LOW (2)	MIDDLE (3)	HIGH (4)
Hardware (Electronic / Electrical)	FFF replacement of discrete component(s) (e.g. resistors, capacitors) where all failures modes are clearly identified in Annex C of EN 50129 Modification of simple electrical component(s) (e.g. lights, horns)	Removal / addition of discrete component(s) (e.g. resistors, capacitors) where all failures modes are clearly identified in Annex C of EN 50129 Small modification on the PCB Modification of complex equipment (s) (e.g. EMC filter)	Re-design / new PCB (i.e. defined in adequacy to EN 50124) Modification of complex electrical equipment(s) (e.g. power supply, fans)	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
Software	- Results from the SPPRAMSS-13903 analysis - 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 - No internal or external interface impacted - Coding standards (from Table A.12 from SPPRAMSS-8814 - [EN 50716:2023] are defined and respected	- Results from the SPPRAMSS-13903 analysis - 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 - No external interface impacted (within the building block) - All impacted interfaces are fully described - Coding standards (from Table A.12 from SPPRAMSS-8814 - [EN 50716:2023] are defined and respected	- Results from the SPPRAMSS-13903 analysis - 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 - External interface(s) impacted (within the building block) - Impacted interfaces are not fully described - Coding standards (from Table A.12 from SPPRAMSS-8814 - [EN 50716:2023] are defined and respected	- Results from the SPPRAMSS-13903 analysis - 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 - External interface(s) impacted (outside the building block) - Impacted interfaces are not described - Coding standards (from Table A.12 from SPPRAMSS-8814 - [EN 50716:2023] are defined and respected

Complexity	MINIMAL (1)	LOW (2)	MIDDLE (3)	HIGH (4)
Technical file (i.e. documentation used for the assessment) Note: testing are not considered as DESIGN documents	Weak 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 RAILWAY OPERATION 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)
Operation, installation, commissioning, and maintenance	No impact on operation, installation, commissioning and maintenance	- 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) that can impact only indirectly safety according to EN50129 §6.3. - More resources due to the higher complexity (e.g. more time required) - Modification / addition of AC(s)	-New Software/Tool needed (e.g. new service Sw, new laptop, new Hw tool) that can impact safety according to EN50129 §6.3. - Modification of the facilities (e.g. train depot, new tests equipments) - Creating new processes (e.g. new testing/validation process)

The Complexity Score is the highest value reached by one of the lines.

If several lines reach this value, an additional expert judgement is needed.

ID	SPPRAMSS-1241
Type	System Requirement

Software Complexity Metrics
Metrics shall be used for SIL1 to SIL4 and documented in the Coding Standards to determine the level of Complexity (MINIMAL / LOW / MEDIUM / HIGH).
Documentation shall include threshold values, and means of enforcement.
As the metrics are specific to each programming languages, the metrics will not be defined in the document. Some examples are described in SPPRAMSS-13902 - Software Complexity Criteria.

ID	SPPRAMSS-13903
Type	System Requirement

Promotion of software metrics
In the current version of the standard SPPRAMSS-8814 - [EN 50716:2023], the deployment of metrics (i.e. Table A.5) is only Recommended. However, in the context of evolution management of safety-related modular systems it needs to be acknowledged that metrics have a higher importance and therefore, should be at least Highly Recommended. **[**SPPRAMSS-13912, Rationale **]**

Complexity criteria to be updated in a next revision
Mechanical evolutions shall be taken into account for the Complexity criteria.
For example : Necessary time to replace / modify the building block ?

To analyse in SC2.5, after discussions with TrainCS.
[SPPRAMSS-8884, Issue, Open, Markus Spindler (Rail Expert Consult) **]**

4.4.2.5 Monitoring

Monitoring
The Monitoring criterion is defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] as follow:
(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;

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

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

The Monitoring of the evolution shall be analysed.

Table 9 Management of Monitoring criterion

Monitoring	MINIMAL (4)	LOW (3)	MIDDLE (2)	HIGH (1)
Is the evolution monitored?	- No failure detection at all. The evolution is not monitored. - The failures are visible in commercial service, only after they take effect / impact commercial service. - Not detectable during preventive maintenance	- The failure is not automatically detected but the system reacts automatically. - The failure is detected by the maintainer after it occurs during depot checks (e.g. periodic maintenance checks) - There is no code nor information point that a failure has occurred - Detectable during preventive maintenance	- The failure is automatically detected and the system **does not react** automatically. - The failure is detected by the maintainer after it occurs during depot checks (e.g. periodic maintenance checks) - **There is a information point** that a failure has occurred - Detectable during preventive maintenance	- The failure is automatically detected and the system reacts automatically. - Hardware potential failures are detected before they could happen (i.e. preditctive maintenance) - Detected prior thanks to Predictive Maintenance

ID	SPPRAMSS-1239
Type	System Requirement

4.4.2.6 Reversibility

Reversibility
The Reversibility criterion is defined in SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] as follow:
(e) reversibility: the inability to revert to the system before the change;

The Reversibility refers to the retrofit of the SuC into a previous certified version.

The Reversibility shall be analysed.

Table 10 Management of Reversibility criterion

Reversibility	MINIMAL (4)	LOW (3)	MIDDLE (2)	HIGH (1)
Is the evolution reversible ?	The retrofit to a previous version is not possible. It requires the re-design of the LRU	A retrofit is possible but requires the replacement of a SRU (by the supplier)	A retrofit is possible but need a manual intervention on-site : - replacement of the LRU - downgrade of the LRU	Automatic / Remote software downgrade is possible to retrofit.

ID	SPPRAMSS-5671
Type	System Requirement

4.4.2.7 Urgency

Urgency Criteria
The Urgency criterion is defined as the necessity to deploy faster an evolution than normally in case of a very high and probable RAM or safety issue. For example :

- a bug in a SIL4 software that prevents the train from running.
- a cyber-security issue easily exploitable that could could affect SIL4 functions.
- a very common bug in a SIL2 function that could have SIL2 consequences.

The RAM, financial and safety consequences of the initial problem shall be analysed.
The result of the analysis shall be used as "bonus points" which purposes is to decrease the safety score.
The analysis shall not take into account how the modification will be made (considerations like impact on BIL or SIL functions).

Table 11 Management of Urgency criterion

Urgency	MINIMAL (4)	LOW (3)	MIDDLE (2)	HIGH (1)
RAM impact	No significant effect on reliability, availability, or maintainability. Service remains largely unaffected with very rare interruptions.	Minor effects on one or more RAM aspects. Service is slightly affected but remains largely reliable. Minor inconveniences to passengers or staff.	Moderate effects on one or more RAM aspects. Service is noticeably affected with moderate disruptions. Requires increased maintenance and resources.	Significant effects on one or more RAM aspects. Major disruptions to service, reliability, or availability. High resource demands for maintenance and issue resolution.
Financial impact	Impact not visible on annual basis	Impact in a significant way the organisation annual benefits.	Impact in a significant way the organisation annual budget (>10 % of revenue)	Could lead to the organisation bankrupcy
Safety impact	No injuries	Highly probable Slight injuries	Highly probable Severe Injuries / 1 single Death	Highly probable Several Deaths

The Urgency Score is determined by the smallest number (where 1 is the highest urgency and 4 is the lowest).
1 = High Urgency (most severe impact)
4 = Minimal Urgency (least severe impact)

ID	SPPRAMSS-8815
Type	System Requirement

4.4.3 Combination of criteria in the Significance Matrix

Combination of criteria
When all criteria have been quantified, their values shall be reported in the SPPRAMSS-8885 - Significance Matrix .

The Significance matrix takes inspiration from the Safety Significance Analysis from SPPRAMSS-9691 - [EN 17023: 2018] , which provides two examples of combinations (refer to Figure A.2).
Based on the result of the seven 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, test and homologate the evolution.

ID	SPPRAMSS-8168
Type	System Requirement

Significance Matrix

Table 12 Significance Matrix

KPI	Minimal	Low	Middle	High
Additionality	1	2	3	4
Failure Consequence	1	2	3	4
Innovation/novelty	1	2	3	4
Complexity	1	2	3	4
Monitoring	4	3	2	1
Reversibility	4	3	2	1
Urgency	4	3	2	1

ID	SPPRAMSS-8885
Type	System Requirement

Significance Score
The data from the Significance Matrix shall then be combined to calculate a Significance Score.

The Formula is the Following :

Significance Score = Additionality Score + Failure Consequence Score + Innovation/Novelty Score + Complexity Score + Monitoring Score + Reversibility Score + Urgency Score.

ID	SPPRAMSS-8886
Type	System Requirement

Levels of Significance
The Significance Score shall then be used to determine the Level of Significance of the evolution according to the following table :

Table 13 Significance Score

Significance Score	Level of Significance
Score = 7	MINIMAL
7 < Score < 14	LOW
14 <= Score < 21	MEDIUM
Score >= 21	HIGH

ID	SPPRAMSS-8889
Type	System Requirement

Nota : Explanation of the Significance Score calculation
The minimum possible Significance Score is 7.
The maximum possible Significance Score possible is 28.

The Minimal Significance is equal to the minimum possible score : 7.
The limit between Low Significance and Medium Significance is equal to 50% of the maximum possible

score : 0,5 * 28 = 14.
The limit between the Medium Significance and the High Significance is equal to 75% of the maximum possible score = 0,75 * 28 = 21. **[**SPPRAMSS-9886, Text **]**

4.4.4 Shortcuts to the Significance Process

Shortcuts to the Significance Process
In some cases, it is not necessary to perform the Significance Process.
Several shortcuts are defined below. **[**SPPRAMSS-15257, Text **]**

Level of Significance of an error correction in the source code
The Level of Significance of an error correction in the source code deviating from intended functions and/ or performance, as described in SPPRAMSS-14396 - Error correction , is MINIMAL.

ID	SPPRAMSS-14398
Type	System Requirement

Level of Significance of a cyber-security-related evolution not impacting / interfering with safety
The Level of Significance of an a cyber-security-evolution not impacting / interfering with safety, as described in SPPRAMSS-15348 - Cyber-security and Significance , is MINIMAL.

ID	SPPRAMSS-16557
Type	System Requirement

Level of Significance of an external interface of the Building Block
The Level of Significance in case of a modification of an external interface is HIGH.

ID	SPPRAMSS-15255
Type	System Requirement

4.4.5 Examples

Normal process
Let's consider a bug fix on a SIL2 software correcting a RAM issue that could have a low RAM impact (No Urgency):
We analyse each criterion and affect it from MINIMAL to HIGH.

KPI	Minimal	Low	Middle	High
Additionality	1	2	3	4
Failure Consequence	1	2	3	4
Innovation/novelty	1	2	3	4
Complexity	1	2	3	4
Monitoring	4	3	2	1
Reversibility	4	3	2	1
Urgency	4	3	2	1

Significance Score = 1 +1 +1 +1 +1+ 1+ 3 = 9

The Level of Significance is LOW. **[**SPPRAMSS-5673, Text **]**

Fast process with a RAM issue
Let's consider a bug fix on a SIL2 software correcting a RAM issue that could have a HIGH RAM impact (Urgency) :
We analyse each criterion and affect it from MINIMAL to HIGH.

KPI	Minimal	Low	Middle	High
Additionality	1	2	3	4
Failure Consequence	1	2	3	4
Innovation/novelty	1	2	3	4
Complexity	1	2	3	4
Monitoring	4	3	2	1
Reversibility	4	3	2	1
Urgency	4	3	2	1

Significance Score = 1 +1 +1 +1 +1+ 1+ 1 = 7

The Level of Significance is MINIMAL.
[SPPRAMSS-9882, Text **]**

Fast Process with a SIL4 consequence of the issue
Let's consider a bug fix on a SIL4 software correcting a Safety issue that could have a HIGH Safety impact (Urgency) :
We analyse each criterion and affect it from MINIMAL to HIGH.

KPI	Minimal	Low	Middle	High
Additionality	1	2	3	4
Failure Consequence	1	2	3	4
Innovation/novelty	1	2	3	4
Complexity	1	2	3	4
Monitoring	4	3	2	1
Reversibility	4	3	2	1
Urgency	4	3	2	1

Significance Score = 1 + 4 +1 +1 +1+ 1+ 1 = 10

The Level of Significance is LOW. **[**SPPRAMSS-9883, Text **]**

Source code deviating from its intended functions and/or performance
Let's consider an error correction in the source code of a SIL4 software deviating from its intended functions and/or performance.
We apply a simplified process : we don't analyse each criterion.

The Level of Significance is MINIMAL. **[**SPPRAMSS-14399, Text **]**

Patch of a cyber-security-related software component not impacting / interfering with safety-related functions
Let's consider a patch of a cyber-security-related software component that does not impact / interfere with safety-related functions.
As defined in the the SPPRAMSS-15348 - Cyber-security and Significance : the Evolution Management process is not applicable, the cyber-security process is applicable.

The Level of Significance is MINIMAL. **[**SPPRAMSS-16555, Text **]**

4.5 Software development process

General aspects
For safety related software, SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] requires the use of SPPRAMSS-8814 - [EN 50716:2023] or equivalent measures.
It is important to note that standard SPPRAMSS-8814 - [EN 50716:2023] makes it possible to reduce the risk of software failures affecting the PRAM aspects of railways, because they impose controlled methods, organisations, tools and metrics. **[**SPPRAMSS-13910, Text **]**

Software development process for initial release
All railways related software (i.e. covering a railway function identified in EN 15380-4) shall be developed at least according to BIL requirements from SPPRAMSS-8814 - [EN 50716:2023].
Note: software that complies with rules for "pre-existing software" defined in SPPRAMSS-8814 - [EN 50716:2023] faces relaxed requirements.

ID	SPPRAMSS-13905
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Segregation between railway and non-railway software
All software implementing non-railway functions, where non-interference between non-railway functions (i.e. general use) and railways functions (e.g. identified in EN 15380-4) cannot be demonstrated, shall be developed at least according to BIL requirements from SPPRAMSS-8814 - [EN 50716:2023].
Note: software that complies with rules for "pre-existing software" defined in SPPRAMSS-8814 - [EN 50716:2023] faces relaxed requirements.

ID	SPPRAMSS-13907
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 CONEMP, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Application Data
Any application data shall be developped according to the SPPRAMSS-8814 - [EN 50716:2023] (chapter 8 "Development of application data: systems configured by application data").

This includes the data specified by the WG Transversal CCS in TCCS CONEMP - Configuration and Diagnostics.

ID	SPPRAMSS-15550
To be derived by Team	SP Task 2 TrafficCS, SP Task 2 Train CS, SP Task 2 Trackside Asset CS, SP Task 2 CONEMP, SP Task 2 CONEMP Computing Environment
Type	System Requirement

Rationale on Application Data
By "application data", the SPPRAMSS-8814 - [EN 50716:2023]understands data which enables the customisation of approved generic software to meet the specific needs of each installation. Its correct derivation and validation ensure the intended behaviour of the system. Since application data directly configures safety-related functions (e.g. signalling logic, door closing timings), its development must follow the same structured process and assessment as software to guarantee safety and consistency across installations. **[**SPPRAMSS-15663, Rationale **]**

Competence of the organisation evolving the SuC
There are missing evidences for organisational competences for BIL Software.
The PRAMS team shall think of criteria/rules to reinforce the competences check for an organisation building BIL Sw. This is too vague and not mandatory checked inside SPPRAMSS-8814 - [EN 50716:2023].

In the next contract, the following ideas shall be analysed :

- EN50716 - Process and organisation audit of the teams in charge of BIL software by an ISA (initial audit + regular checks, frequency to be determined)
- Get inspiration from the Safety Management Systems certifications.
- Analyse the IRIS certification regarding Software
- The organisation in charge of operating the software shall also be checked regularly. Hint : the software is developped and operated by 2 different organisations.

[SPPRAMSS-13908, Issue, Open, Markus Spindler (Rail Expert Consult) **]**

Re-use of widely deployed COTS
To avoid facing important PRAM issues when using COTS, PRAMS team shall propose rules, hints, conditions to allow or not the use of well deployed COTS outisde railway market for CCS purpose. This case will pop-up very soon when dealing with the Computing Platform (e.g. generic BIL or "not-BIL" Hw, on the shelf OS like Linux...). We need to ensure that these reuses will not jeopardize PRAM requirements (to be defined later) for the overall CCS systems.
Hints: analyse the EN50716 50129 50126 50155 requirements an OCORA-BWS09-020_Acceptance-of-Global_Standards_Focus-on-Safety-in-CCS about COTS Software and Hardware. **[**SPPRAMSS-13909, Issue, Open **]**

Input for STIP
We need to ask into the STIP to :

- update this requirement of §4.4 of SPPRAMSS-8814 - [EN 50716:2023] to ensure a minimum PRAM level in railway software -> the BIL requirements shall be mandatory for any software dealing with a function identified in EN 15380-4.
- SPPRAMSS-13912 - Promotion of software metrics should also be included.

As an exemple, take inspiration by this Change Request written by TrainCS :
CR-11913-Ethernet_CCS_Consist_Network **[**SPPRAMSS-13906, Issue, Open **]**

Software development process for evolutions
Although it is mainly dedicated to new developments, the SPPRAMSS-8814 - [EN 50716:2023] is highly recommended to be used for software evolutions. Therefore, it is widely used by the industry for such purposes.

Two types of evolutions are listed in the SPPRAMSS-8814 - [EN 50716:2023] standard:

- minor
- major

For a major evolution, the SPPRAMSS-8814 - [EN 50716:2023] shall be applied in its entirety.
For a minor evolution only one chapter of the the SPPRAMSS-8814 - [EN 50716:2023] shall be applied : §9.2 “Software Maintenance”, which allows to use a much lighter process of development.

In the context of Europe's Rail, a minor evolution should require the strict minimal effort, but should contain at least the documentation required for Basic Integrity as presented in SPPRAMSS-10088 - Documentation list for minor software modifications .

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 currently 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 a SIL1-4 software developed according to the SPPRAMSS-8814 - [EN 50716:2023]

As the the SPPRAMSS-8814 - [EN 50716:2023] do not define what is a minor and a major evolution and it can be difficult to define it.

This is why the present document proposes the following process. **[**SPPRAMSS-5675, Text **]**

Significance Impact and Software development process
After having determined if a modification has a MINIMAL, LOW, MIDDLE or HIGH Level of Significance, the supplier shall use the following table:

Table 14 Corresponding table between Significance Impact and Software modification process

Level of Significance of the software evolution	Type of software modification according to §9.2 of the SPPRAMSS-8814 - [EN 50716:2023]	Software modification process to apply (according to §9.2 of the SPPRAMSS-8814 - [EN 50716:2023])
MINIMAL	minor	Application of the previously defined maintenance methods by the building block documentation (refer to SPPRAMSS-10088 - Documentation list for minor software modifications) Application of the strict minimal effort : at least the documentation required for Basic Integrity shall be realised.
LOW	minor	Application of the previously defined maintenance methods by the building block documentation (refer to SPPRAMSS-10088 - Documentation list for minor software modifications) Application of the strict minimal effort : at least the documentation required for Basic Integrity shall be realised.
MIDDLE	minor or major	No generic position regarding minor or major type of change is possible. The user shall make its own arbitration based on contextual data.
HIGH	major	Use a full development process defined by SPPRAMSS-8814 - [EN 50716:2023]

ID	SPPRAMSS-5676
Type	System Requirement

Software Documentation and Additionnality
If the Additionnality criteria is **HIGH**, all the documents describing the evolutions made since the last valid ISA certificates shall be integrated in the genuine documentation requested by the SPPRAMSS-8814 - [EN 50716:2023] (e.g. Software Requirements Specification, Software Interface Specification, ...).

This is requested to avoid potential side effects of managing too many evolutions, without updating the original documentation.

ID	SPPRAMSS-10089
Type	System Requirement

Documentation list for minor software modifications
In the context of the future modular architecture, the following list of documents shall be provided by the building block suppliers / integrators as minimum mandatory artefacts related to a minor evolution for all building blocks (independent from their BIL/SIL). This is defined in section 9.2 of SPPRAMSS-8814 - [EN 50716:2023] for a software in maintenance phase :

- Software Maintenance Plan
- Software Change Records
- Software Maintenance Records
- Software Maintenance Verification Report

Note: the content expected from each document is recapped hereafter:

- **1) Software Maintenance Plan**
  - 9.2.4.5 A Software Maintenance Plan shall be written on the basis of the input documents from 9.2.2. The requirement 9.2.4.6 refers to the Software Maintenance Plan.
  - 9.2.4.6 Procedures for the maintenance of software shall be established and recorded in the Software Maintenance Plan. These procedures shall also address
    - a) control of error reporting, error logs, maintenance records, change authorization and software/system configuration and the techniques and measures in Table A.10,
    - b) verification, validation and, for SIL 1 to SIL 4, assessment of any modification,
    - c) definition of the Authority which approves the changed software, and
    - d) authorization for the modification.
  - 9.2.4.12 Once the Software Maintenance Plan has been established, verification shall address
    - a) that the Software Maintenance Plan meets the general requirements for readability and traceability in 5.3.2.7 to 5.3.2.10 and in 6.5.4.14 to 6.5.4.17 as well as the specific requirements in 9.2.4.6,
    - b) the internal consistency of the Software Maintenance Plan.
  - 9.2.4.15 The maintenance activities shall be carried out following the Software Maintenance Plan to the extent required by the software integrity level
- **2) Software Change Records**
  - 9.2.4.9 A Software Change Record shall be written on the basis of the input documents from 9.2.2. The requirement in 9.2.4.10 refers to the Software Change Record.
  - 9.2.4.10 A Software Change Record shall be established for each maintenance activity. This record shall include
    - a) the modification or change request, version, nature of fault, required change and source for change,

        - b) an analysis of the impact of the maintenance activity on the overall system, including hardware, software, human interaction and the environment and possible interactions,
        - c) the detailed specification of the modification or change carried out, and
        - d) revalidation, regression testing and re-assessment of the modification or change to the extent required by the software integrity level. The responsibility for revalidation can vary from project to project, according to the software integrity level. Also the impact of the modification or change on the process of revalidation can be confined to different system levels (only changed components, all identified affected components, the complete system). Therefore the Software Validation Plan shall address both problems, according to the software integrity level. The degree of independence of revalidation shall be the same as that for validation.

    - 9.2.4.14 Once the Software Change Record has been established, verification shall address

        - a) that the Software Change Record meets the general requirements for readability and traceability in 5.3.2.7 to 5.3.2.10 and in 6.5.4.14 to 6.5.4.17 as well as the specific requirements in 9.2.4.10,
        - b) the internal consistency of the Software Change Record.

- **3) Software Maintenance Records** (refer to SPPRAMSS-10090 - Software Change Records)

    - 9.2.4.7 A Software Maintenance Record shall be written on the basis of the input documents from 9.2.2.
    - 9.2.4.8 A Software Maintenance Record shall be established for each software item before its first release, and it shall be maintained. The Maintenance Record shall include

        - a) references to all the Software Change Records for that software item,
        - b) change impact evaluation,
        - c) test cases, including revalidation and regression testing data, and
        - d) software configuration history.

    - 9.2.4.13 Once the Software Maintenance Record has been established, verification shall address

        - a) that the Software Maintenance Record meets the general requirements for readability and traceability in 5.3.2.7 to 5.3.2.10 and in 6.5.4.14 to 6.5.4.17 as well as the specific requirements in 9.2.4.8,
        - b) the internal consistency of the Software Maintenance Record.

- **4) Software Maintenance Verification Report**

    - 9.2.4.11 A Software Maintenance Verification Report shall be written, under the responsibility of the Verifier, on the basis of the input documents from 9.2.2.
    - Requirements from 9.2.4.12 to 9.2.4.14 refer to the Software Maintenance Verification Report

The following general requirements from SPPRAMSS-8814 - [EN 50716:2023]are applicable to the above list of mandatory documents:

- 5.3.2.7 For each document, traceability shall be provided in terms of a unique reference number and a defined and documented relationship with other documents.
- 5.3.2.8 Each term, acronym or abbreviation shall have the same meaning in every document. If, for historical reasons, this is not possible, the different meanings shall be listed and the references given.
- 5.3.2.9 Except for documents of the pre-existing software (see 7.3.4.7), each document shall be written according to the following rules:

    - it shall contain or implement all applicable conditions and requirements of the preceding document with which it has a hierarchical relationship;
    - it shall not contradict the preceding document.

- 5.3.2.10 Each item or concept shall be referred to by the same name or description in every document. Sw quality elements applicable to the 4 above documents:

The following software quality requirements from SPPRAMSS-8814 - [EN 50716:2023]are applicable to the above list of mandatory documents:

- 6.5.4.14 Traceability to requirements shall be an important consideration in the validation of the system and means shall be provided to allow this to be demonstrated throughout all phases of the lifecycle
- 6.5.4.15 Within the context of this document, and to a degree appropriate to the specified software integrity level, traceability shall particularly address
  - a) traceability of requirements to the design or other objects which fulfil them,
  - b) traceability of design objects to the implementation objects which instantiate them,
  - c) traceability of requirements and design objects to the tests (component, integration, overall test) and analyses that verify them.
  - Traceability shall be the subject of configuration management.
- 6.5.4.16 In special cases, e.g. pre-existing software or prototyped software, traceability may be established after the implementation and/or documentation of the code, but prior to verification/validation. In these cases, it shall be shown that verification/validation is as effective as it would have been with traceability over all phases.
- 6.5.4.17 Objects of requirements, design or implementation that cannot be adequately traced shall be demonstrated to have no bearing upon the safety or integrity of the system.

ID	SPPRAMSS-10088
Type	System Requirement

Software Change Records
As the ERJU is dealing with a standardised modular architecture, the management of the interfaces between the building blocks is a key element. Therefore, the following aspects from the SPPRAMSS-8814 - [EN 50716:2023] shall be systematically mentioned in all impact analyses presented in the "Software Change Records":

- 6. Software Requirements Specification
  - To list all genuine requirements impacted or to be created related to the evolution or,
  - To mention that no requirement is impacted (e.g. implementation bug fixing)
- 11. Software Interface Specifications
  - To list all genuine requirements impacted or to be created related to the evolution
  - To mention that no requirement is impacted (e.g. implementation bug fixing)
- 28. Application Requirements Specifications
  - To list all genuine requirements impacted or to be created related to the evolution
  - To mention that no requirement is impacted (e.g. implementation bug fixing)

Regarding the modifications related to the interoperable components, the "Software Change Records" shall also highlight the absence of modification of any basic parameters or basic design characteristics. These conditions are defined:

- For the CCS-OB integrated system and its building blocks in:
  - SPPRAMSS-7345 - 7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics
  - SPPRAMSS-8058 - 7.2.2.3 Conditions for a change in the On-board mobile communication functions for railways or in the ATO on-board functionality that does not impact the basic design characteristics
  - SPPRAMSS-8061 - 7.2.2.4 Conditions for a change in the on-board...

- For the CCS trackside integrated system and its building blocks in:
  - SPPRAMSS-8080 - 7.2.3.2 Conditions for an upgrade or renewal in the trackside ETCS functionality that, if not fulfilled, requires new authorisation for placing in service
  - SPPRAMSS-8082 - 7.2.3.3 Conditions for an upgrade or renewal in the trackside mobile communication for railways or trackside ATO functionality that, if no fulfilled, requires a new authorisation for placing in service
  - SPPRAMSS-8081 - 7.2.3.4 Impact o the technical compatibility between on-board and trackside parts if the CCS subsystems

ID	SPPRAMSS-10090
Type	System Requirement

4.6 Hardware development process

Hardware development process Introduction
Unfortunately, the software maintenance process defined in SPPRAMSS-8814 - [EN 50716:2023] 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… **[**SPPRAMSS-5677, Text **]**

Hardware development process to create
The evolution management process for hardware development is not defined at the moment and will be defined in a future release of the present document.

It should be defined when the process is relevant for hardware, as much more functions will be virtualised, and there should be an abstraction layer between the function and the hardware bellow.
Maybe only when FFIS are impacted ?

No requirements in EN50155 and EN50129 describing an hardware evolution process, as exisiting in the EN50716 for software (minor / major evolution) were found by the team.

In the Computing Management WG, the hardware evolutions are described only for a high level / operational point of view.

How to deal with such evolution, including interchangeability ?

For sure, EMC and performance testing will ne necessary for hardware evolution, including for intercheangeability of FFF building blocks from different suppliers.

The replacement of COTS by another COTS shall be analysed.

The obsolescence management shall be analysed.

Hints :

- Define use cases with different type of COTS :
  - Railway-specific COTS
  - Non-railway specific but critical industry COTS (avionics, military, medical, ...)
  - Generic purpose COTS
- And check which part of the process are applicable or no

[SPPRAMSS-8873, Issue, Open, Julien Bois, Iñigo Iruretagoyena Tormo **]**

4.7 Testing Process

Test impact process and matrix
The second major step of the overall evolution management process represents the management of the testing activities focusing on the standardised interfaces (refer to SPPRAMSS-5669 - Process point of view the evolution management). This activity is postponed as agreed in SPPRAMSS-9752 - Connection between PRAMS and IP WP34/35 and SPPRAMSS-9693 - Connection between PRAMS and IP FP2 R2DATO WP34/35 Testing. **[**SPPRAMSS-5680, Text **]**

Connection between PRAMS and IP FP2 R2DATO WP34/35 Testing
Until SC2.5, no team dealing with testing activities was built within SP.
The activity of testing shall be started as soon as the first system requirements are defined to initiate the discussion on modular and automatic testing activities.
An official connection has been done between the PRAMS teams and the IP teams dealing with testing activities (i.e. WP33 and WP34). A roadmap shall be defined for remit SC2.6 to see how the two teams can collaborate on the technical topic of testing activities in the context of evolution management.
[SPPRAMSS-9693, Issue, Open, Julien Bois **]**

4.8 Assessment Process

ISA / NoBo / AsBO
The difference between the 3 types of assesments (yLoS / LoS / New certificate) should be better described in this chapter regarding the roles of ISA / AsBo, that have changed in the TSI CCS 2023.

The document should be updated after beeing reviewed by the NB Rail association and the ERA / AsBo cooperation group.

Postponed to SC2.6 after sending the version 2 of the document **[**SPPRAMSS-11467, Issue, Open, Markus Spindler (Rail Expert Consult) **]**

IP FP2 R2DATO WP26 "T26.3. - Study on modular certification and acceptance approaches for Modular Platforms"
The conclusions of the document "T26.3. - Study on modular certification and acceptance approaches for Modular Platforms written by the IP FP2 R2DATO WP26 should be taken into account in the process.

To deal in SC2.6
[SPPRAMSS-14693, Issue, Open, Markus Spindler (Rail Expert Consult) **]**

Linking the System Pillar Reference Architecture with the System breakdown of current European homologation process
The list of Basic Design Characteristics from the SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] shall be updated to reflect the System Pillar Reference Architecture.

For example, at the moment:

- interoperability constituants cover only trackside and onboard components essential for train/track inter-operation
- interlockings are not in the list of interoperability constituents

This should lead to a Change Request, initiated by PRAMS and reviews by TrainCS and TrafficCS in the next contract, as identified by the STIP_81 **[**SPPRAMSS-13896, Issue, Open, Julien Bois **]**

Context of current assessment processes
CCS systems and their constituents are required to be designed in conformity with the CENELEC standards as defined in the Table A.3 of SPPRAMSS-328 - [Commission Implementing Regulation

2023/1695 "TSI CCS"]:

- SPPRAMSS-349 - [EN 50126-1:2017]
- SPPRAMSS-335 - [EN 50126-2:2017]
- SPPRAMSS-336 - [EN 50128:2011 + A2/2020]
- SPPRAMSS-334 - [EN 50129:2018/AC:2019-04]
- Note: SPPRAMSS-8035 - EN50716 instead to replace SPPRAMSS-336 - [EN 50128:2011 + A2/2020] in the future for any railway software development

Finally:

- The NoBo will issue for each CCS OB constituent a "EC Design examination certificate" (based on the type of module assessment defined in SPPRAMSS-9953 - [Decision (EU) 2010/713]) which ensures that the systems meets all basic parameters and basic design characteristics,
- The AsBo (previously done by an ISA in TSI CCS: 2016) will issue an AsBo certificate wich ensures that the system meets the CENELEC requirements SPPRAMSS-349 - [EN 50126-1:2017], SPPRAMSS-335 - [EN 50126-2:2017], SPPRAMSS-336 - [EN 50128:2011 + A2/2020], SPPRAMSS-334 - [EN 50129:2018/AC:2019-04], SPPRAMSS-8035 - EN50716 for the claimed SIL (i.e. SIL1 to SIL4). No certificate is issued for BIL systems.

Today, neither the SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] nor the CENELEC standards define what can be done in case of "minor" modifications on a CCS system. Therefore, some companies have defined process to cover such cases with accredited assessors to avoid requesting a new certificate for minor updates. These solution are companies or products specific and can be challenged when a different assessor (from the one who validates this process) is involved.

Regarding the changes related to interoperability, a status has been provided in section SPPRAMSS-8051 - Change management in TSI CCS 2023. However, when a change does not meet the conditions defined in SPPRAMSS-7345 - 7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics, it means that a new NoBo assessment is required although the change can be "minor".

Based on the result of the standardised analysis of evolutions defined in section SPPRAMSS-8173 - Evolution Management process, the PRAMS team defined three levels of assessments. This covers both CENELEC and/or TSI assessments. They have been defined in respect with the safety and interoperable regulations and without degrading the overall safety level or interoperability. **[**SPPRAMSS-9754, Text **]**

4.8.1 No assessment activities

No assessment activities
As the scope of the document is systems compliant to SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"], this possibility exist only for evolutions of a software component **which is not** implementing or interfering with or impacting a railway function and where an evolution is covered by an adequate code of practice.

ID	SPPRAMSS-9955
Type	System Requirement

4.8.2 Yearly Letter of Support

Yearly Letter of Support (yLoS)
Context:
According to SPPRAMSS-8167 - Safety Assessment matrix and SPPRAMSS-14398 - Level of Significance of an error correction in the source code, this type of assessment can only be used in case:

- The evolution(s) is (are) brought into a BIL and/or interoperable (see SPPRAMSS-11466 - TSI CCS conformity matrix) system (refer to SPPRAMSS-1150 - Separation rules in the building blocks),

- The evolution(s)is (are) patches without any safety impact, on a BIL or SIL system.
- The evolution(s) fulfil(s) the conditions defined in SPPRAMSS-7345 - 7.2.2.2 Conditions for a change in the On-board ETCS functionality that does not impact the basic design characteristics or SPPRAMSS-8080 - 7.2.3.2 Conditions for an upgrade or renewal in the trackside ETCS functionality that, if not fulfilled, requires new authorisation for placing in service .
- The evolution is an SPPRAMSS-15261 - Error correction

A yLoS can be delivered only after a first ISA certificate and/or NoBo Design examination certificate has been issued.

A yLoS can only be delivered to applicants approved by ERA or a NSA to realise evolutions according to SPPRAMSS-619 - [Commission Implementing Regulations 402/2013 "CSM RA" + 2015/1136] , SPPRAMSS-349 - [EN 50126-1:2017] , SPPRAMSS-335 - [EN 50126-2:2017] and in case of software : SPPRAMSS-8814 - [EN 50716:2023] .

Content:
The activities consist for the supplier of the building block or CCS integrated system to follow its internal quality management process to handle evolutions covered by a yLoS.

The documentation shall be updated after each modification covered by a yLoS and saved in the suppliers' records. As these versions are not directly assessed (CENELEC or NoBo), this documentation shall list all versions deployed in commercial revenue and provide for each of them a release note presenting the list of change requests implemented and the reference and version of all modified documents.

Tasks:
The building block supplier shall provide each year to the assessor(s) this file and if requested, any evidence of correct implementation of a change request (e.g. test report, design evidence). This exchange is initiated by the supplier without request from the assessor(s).

The assessor shall be allowed to yearly check the documentation and the source code and audit the supplier.
If the quality level is judged as sufficient, he shall provide an update of the last valid certificate(s) including all the new versions covered by the yLoS.

ID	SPPRAMSS-9956
Type	System Requirement

Rationale for Yearly Letter of Support (yLoS)
The yLoS is an instrument to express the necessary trust in the fitness of an organisation to perform evolution tasks of up to LOW significance on a given building block.
The ISA/AsBo issuing the letter of support needs to define the extent of this trust, according to his assessment of the building block, the organisation and the previous work of that organisation.
To this aim, the ISA / AsBo names the versions / version range of the building block for which the yLoS is applicable, a time range for which the yLoS is valid and after which a new yLoS is necessary, and defines a threshold maximum value of error corrections for which the yLoS gives support and any other threshold or criterion the ISA / AsBo deems necessary. **[**SPPRAMSS-15264, Rationale **]**

Rationale on Additionality in case of error correction
The residual error rate refers to the number of error which could not be detected throughout the verification and validation activities during the building block development (i.e. even in SIL4 system 100% of test coverage against space of system states is not possible and not requested by the CENELEC standards).

Understanding the residual error rate, and its acceptable values in relation to the targeted Software Integrity Level, supports controlling the number of error-correction modifications that may occur after an ISA certificate (covering CENELEC standards) has been issued. This requirement is assigned to the assessor, who is best placed to evaluate it due to their expertise in the complexity of the building block and the robustness of the supplier’s organisation.

If the threshold (i.e. maximum number of error-correction modifications) is exceeded, the yLoS no longer permits additional error corrections to be performed under its scope. This situation may arise for two main reasons:

1. **Misclassification of changes** – Regular evolutions are mistakenly recorded as error corrections. In this case, the organisation must refine its criteria for identifying error corrections and reach an agreement with the ISA/AsBo on the revised approach.
2. **Excessive residual error rate** – The SuC must be further investigated to determine whether code quality improvement measures are required for some or all components. This could lead to a maintenance release, or, if the number of errors indicates that the intended Integrity Level defined in the certificate has not been achieved, to the revocation of the ISA/AsBo certificate.

Example on the implementation of the requirement:

- Building block x :
  - Maximum residual error rate: 10
  - Whenever the building block supplier goes beyond 10 change requests, the latter shall run again the complete significance process.
  - The assessor will then judge if the new corrective version will have to follow:
    - SPPRAMSS-8181 - Letter of Support
    - SPPRAMSS-8178 - New Certificate(s)

[SPPRAMSS-15259, Rationale **]**

STIP - Yearly Letter of Support
It is necessary to update the regulations via the STIP to clarify the use of Yearly Letter of Support defined in SPPRAMSS-9956 - Yearly Letter of Support (yLoS) and SPPRAMSS-16087 - Annex - Yearly Letter of Support .
[SPPRAMSS-14400, Issue, Open, Julien Bois **]**

4.8.3 Letter of Support

Letter of Support (LoS)
Context:
According to SPPRAMSS-8167 - Safety Assessment matrix, this type of assessment applies to safety critical systems or interoperable constituents (refer to SPPRAMSS-1150 - Separation rules in the building blocks).

A Letter of Support shall be issued :

- for SIL1 to SIL2 impacted function(s) if the Significance Score of the evolution is < 21.
- for SIL3 to SIL4 impacted function(s) if the Significance Score of the evolution is < 14

Content:
This type of assessment aims at covering minor evolutions thanks to an addendum to the last valid certificate. The quantification of “minor” is the purpose of the significance matrix defined in section SPPRAMSS-8173 - Evolution Management process. The letter of support represents a "delta" assessment focusing on the evolution itself in the building block or integrated CCS system without a re-assessment of the already certified non modified parts. Finally, the last valid CENELEC and/or NoBo certificate(s) remain valid.

This "delta" assessment is represented by the “supplemented by additional documentation” mentioned by SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] in SPPRAMSS-9958 - EN50129: 2018 - §8.3 Modification and retrofit .
The set of documents used to implement the evolution(s) shall be based on a tailored V cycle from

SPPRAMSS-335 - [EN 50126-2:2017] with at least the following documents:

- Impact analysis document based on the current evolution management process or equivalent
- Design document (e.g. specification, architecture, design)
- Implementation evidence (e.g. test code extract, bill of material)
- Testing document (e.g. one or several levels of testing depending on the evolution(s))
- A verification report according to the supplier's quality management system
- A validation report according to the supplier's quality management system
- A safety report covering all above documentation
- A release note presenting all change requests closed with the evolution(s).

Tasks:
To be eligible for a LoS, the building block or CCS system supplier shall provide to the assessor(s) all above documentation or any additional evidence required by the assessor(s).

If the impact analysis is accepted by the assessor(s), the assessment shall focus on the new set of documents only and consider that the original technical file remains valid and is not compromised by the "delta" documentation.
After investigation, the assessor(s) shall provide a addendum to the last valid certificate(s) which claim that the new version can be safety deployed without compromising the last genuine system.

ID	SPPRAMSS-9957
Type	System Requirement

EN50129: 2018 - §8.3 Modification and retrofit
The Letter of support has been defined in respect with §8.3 of SPPRAMSS-334 - [EN 50129:2018/AC:2019-04]. **[**SPPRAMSS-9958, Text **]**

4.8.4 New Certificate(s)

New certificate(s)
Context:
A new AsBo/NoBo certificate is required in case:

- for SIL1 to SIL4 functions impacted by a "high impact" evolution(s).
- for SIL4 functions impacted by a "medium impact" evolution(s).
- the SPPRAMSS-1173 - Additionality in case of evolution Score emitted for the SuC is HIGH
- ERA or a NSA requests it

Content:
This represents a full assessment regarding the CENELEC standards (i.e. new safety case) and/or a new demonstration of compliance regarding the basic parameters (refer to SPPRAMSS-8050 - Basic parameters).

Tasks:
The supplier shall provide all design evidences that the building block or CCS system fulfils all requirements from CENELEC standards and SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"].

The assessor(s) will deliver after investigations:

- **For the NoBo**: a new "EC Design examination certificate" (basic on the type of module assessment defined in SPPRAMSS-9953 - [Decision (EU) 2010/713]) for the new version of the building block or CCS system and/or
- **For the AsBo**: a new AsBo report for the new version of the building block or CCS system.

ID	SPPRAMSS-9959

Type	System Requirement

4.8.5 Safety Assessment matrix

Safety Assessment matrix
When the SPPRAMSS-8886 - Significance Score is defined, the following table shall be used to select the type of safety assessment in accordance with the SPPRAMSS-1234 - Failure consequence of the functions impacted by the evolution.

Table 15 Safety Assessment Matrix

Significance Score	Level of Significance	Minimal Failure Consequence (Basic Integrity)	Middle Failure Consequence (SIL1 / SIL2)	High Failure Consequence (SIL3 / SIL4)
Score >= 21	HIGH	Yearly Letter of Support	New certificate	New certificate
14 <= Score < 21	MEDIUM	Yearly Letter of Support	Letter of Support *	New certificate
Score < 14 **and NOT** SPPRAMSS-14396 - Error correction	LOW	Yearly Letter of Support	Letter of Support *	Letter of Support *
Score < 14 **and** SPPRAMSS-14396 - Error correction	MINIMAL	Yearly Letter of Support	Yearly Letter of Support	Yearly Letter of Support

Table 16 Safety Assessment matrix

* in case the SPPRAMSS-1173 - Additionality in case of evolution Score emitted for the SuC is HIGH or ERA / a NSA requests it, a new certificate shall be delivered.

Note: For cyber-security-related evolutions, refer to:

- SPPRAMSS-14907 - Cyber-Security functionalities
- SPPRAMSS-14908 - Cyber-Security and evolutions of a safety-related software

ID	SPPRAMSS-8167
Type	System Requirement

4.8.6 Assessment at integrated levels

Assessment at integrated levels
Assessment related to the integration of building blocks :

- at sub-system level
- at vehicle / trackside level
- at system level

will be analysed in a future version in the document.
The goal will be to avoid a propagation of assessment activities through the entire integration chain.
[SPPRAMSS-15671, Issue, Open **]**

4.8.7 Assessment activities overview

8.9.6 Assessment activities overview
The Assessment activities overview is presented in the following drawing:

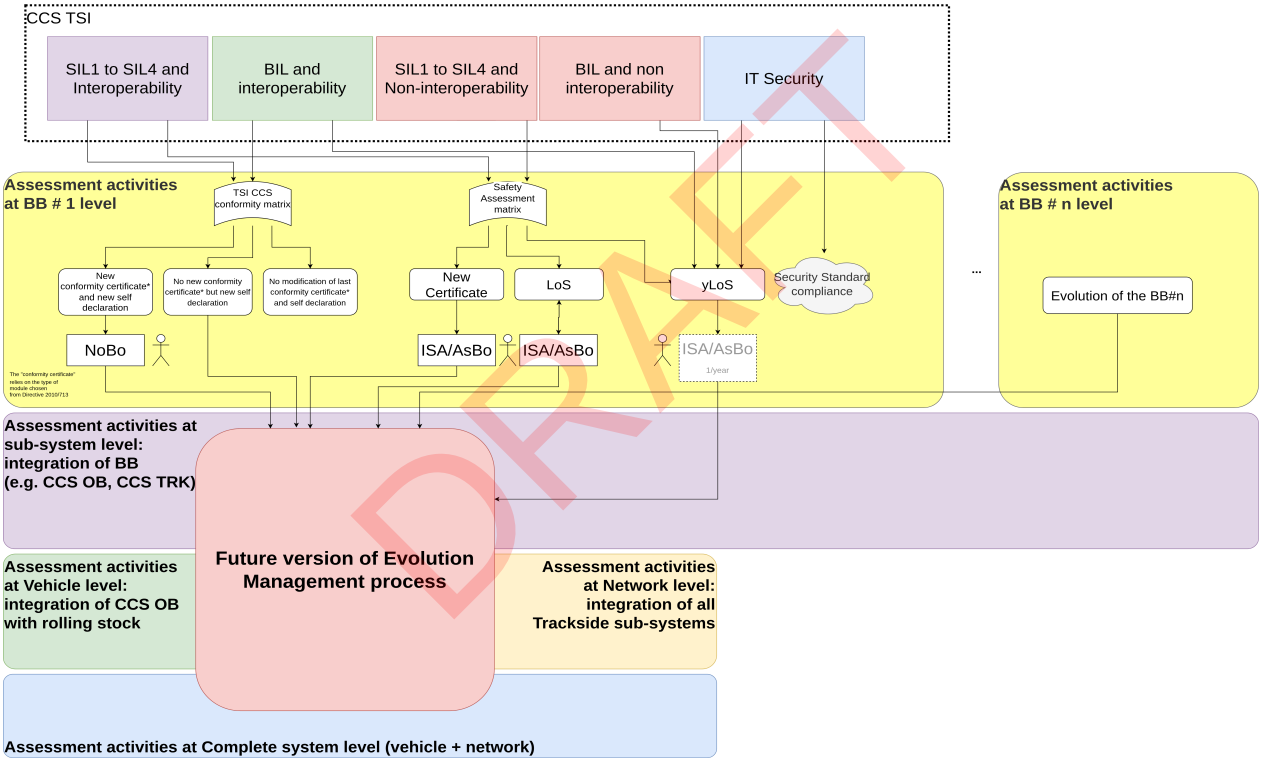


Figure 16 Assessment activities overview

[SPPRAMSS-15669, Text **]**

4.9 TSI CCS conformity process

TSI CCS Conformity process
The current TSI CCS regarding update and renewal of the EC Design Examination Certificate considers safety as one of the input data to determine if an EC Design Examination Certificate is necessary in case of an evolution. This is specified in point 7.2.2.2 or 7.2.3.2 (change of realisation identifier) of SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]. The requirement SPPRAMSS-15665 - Application 7.2.2.2 (3) and 7.2.3.2 (3) of TSI CCS clarifies how the condition 3, linking safety and conformity, has to be evaluated.

The requirement SPPRAMSS-11466 - TSI CCS conformity matrix defines the conditions required to roll-out changes in operation without the need of a new or updated EC Design Examination Certificate.

The requirement SPPRAMSS-15984 - Annual NoBo Assurance Letter defines the concept of continuous supervision of changes which do not need of a new or updated EC Design Examination Certificate.
[SPPRAMSS-15982, Text **]**

Application 7.2.2.2 (3) and 7.2.3.2 (3) of TSI CCS
The SPPRAMSS-8167 - Safety Assessment matrix results shall be used as follows to answer the fulfillment or not of condition 3 of 7.2.2.2 (onboard) or 7.2.3.2 (trackside) of *SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]* (i.e. *(3) The result of the safety judgement (e.g. safety case according to EN 50126) remains unchanged*):

Table 17 Refinement of condition 3

SPPRAMSS-8167 - Safety Assessment matrix results	**Fulfillment of condition 3**
SPPRAMSS-9956 - Yearly Letter of Support (yLoS)	condition 3 of 7.2.2.2 (onboard) or 7.2.3.2 (trackside) is met
SPPRAMSS-9957 - Letter of Support (LoS)	condition 3 of 7.2.2.2 (onboard) or 7.2.3.2 (trackside) is met
SPPRAMSS-9959 - New certificate(s)	condition 3 of 7.2.2.2 (onboard) or 7.2.3.2 (trackside) is not me

ID	SPPRAMSS-15665
Type	System Requirement

Rationale on Application 7.2.2.2 (3) and 7.2.3.2 (3) of TSI CCS
The table from SPPRAMSS-15665 - Application 7.2.2.2 (3) and 7.2.3.2 (3) of TSI CCS allows to link the result of the SPPRAMSS-8167 - Safety Assessment matrix with SPPRAMSS-11466 - TSI CCS conformity matrix. The link between ISA/AsBo and NoBo activities is realised through condition 3 of section 7.2.2.2 or 7.2.3.2 of SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"]. **[**SPPRAMSS-15666, Rationale **]**

TSI CCS conformity matrix
The following table shall be used to select the type of conformity assessment according to SPPRAMSS-4525 - [Directive 2016/797] and SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"].

Table 18 TSI CCS conformity matrix

Changes not impacting the Basic Design Characteristics	Changes impacting the Basic Design Characteristics but inside the acceptable range of parameters	Changes impacting the Basic Design Characteristics and outside the acceptable range of parameters
Fulfilling all the conditions in point 7.2.2.2 or 7.2.3.2 *(change of realisation identifier)* of SPPRAMSS-328 - [Commission Implementing Regulation 2023/1695 "TSI CCS"] with additional criterion defined in SPPRAMSS-15665 - Application 7.2.2.2 (3) and 7.2.3.2 (3) of TSI CCS	Update of the Technical File - no impact on the EC Design Examination Certificate	*Not fulfilling all the conditions in point 7.2.2.2 or* 7.2.3.2 *(change of functional identifier)* Application of the §2.3.3 of SPPRAMSS-4525 - [Directive 2016/797] "2.3.3. In the case of a modification to a subsystem already covered by a certificate of verification, the notified body shall perform only those examinations and tests that are relevant and necessary, i.e. assessment shall relate only to the parts of the subsystem that are changed and their interfaces to the unchanged parts of the subsystem."
Type of NoBo assessment : SPPRAMSS-15984 - Annual NoBo Assurance Letter		Type of NoBo assessment : new EC Design Examination Certificate focusing on the evolution

Table 19 TSI CCS sub-systems conformity assessment matrix

ID	SPPRAMSS-11466
Type	System Requirement

Annual NoBo Assurance Letter
The Annual NoBo Assurance Letter shall formally record the Notified Body's trust in a qualified organisation to perform low-significance evolutions on specified CCS components or building blocks for a period of one year. The organisation shall document all evolutions, versions, and implemented changes, and submit them annually for review.

ID	SPPRAMSS-15984
Type	System Requirement

Rationale on the Annual NoBo Assurance Letter
The Annual NoBo Assurance Letter provides a formal expression of confidence in the organisation's competence, processes, and past performance. It allows minor evolutions to be made without individual assessment, while ensuring annual oversight, traceability, and transparency.

The frequency (1 year) is linked with :

- the annual report requested to maintain valid:
  - the Single Safety Certificate for RUs (article 19 of Commission Implementing Regulation 2016/798)
  - the Safety Authorisation for IMs (article 19 of Commission Implementing Regulation 2016/798)
- the annual reports to be published by:
  - the Investigation Bodies (article 24, point 3 of Commission Implementing Regulation 2016/798)
  - the National Safety Authorities (article 19 of Commission Implementing Regulation 2016/798)
  - the Entities in Charge of Maintenance of vehicles (article 8, point 1 of Commission Implementing Regulation 2019/779)

It deviates on purpose from the 5 year frequency of the certification of Entities in Charge of Maintenance (article 7, point 8 of Commission Implementing Regulation 2019/779), because of the high turnover of software engineers in most of entities.

[SPPRAMSS-15985, Rationale **]**

4.10 Train CS

Allignment with Train CS

Although the document Specification for Authorisation, Integration and Upgradeability of modular train CS system including train interface from TrainCS was reviewed by the PRAMS team and the SPT2TRAIN-3113 - To address the key points according to we suggest the following structure for an... was taken into account, the 2 documents shall be completely in line.

A joint team composed of PRAMS and TrainCS experts shall work on this alignment. **[**SPPRAMSS-11523, Issue, Open, Bois Julien (I-NAT-GST-CCS-EXT - Extern) **]**

5 Update and configuration management

5.1 Introduction

Configuration management is a crucial element for evolution management
One of the major goals of the future modular architecture is to deploy updates on the CCS building blocks in a faster and larger scale as it is realized today. Indeed, in the current CCS integrated systems, updates are most of the time performed manually by the maintainer on each CCS equipment by connecting locally a maintenance computer to the system. One of the major pitfall is the immobilisation (for CCS OB) or unavailability (for CCS trackside) of the consist in case of an update. 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”. **[**SPPRAMSS-1228, Text **]**

Work in the SP Domain Transversal
The SP Domain Transversal has initiated a configuration management process for the future CCS building blocks; on-board and trackside.
This is defined in the documents:

- TCCS Configuration - Operational Epics
- TCCS Configuration - High Level Concept
- TCCS Configuration - System Requirements
- Logical Concept
- TCCS Service Function Configuration (SFC) L5

The PRAMS team has been involved as reviewers for these artefacts.
The listed documents will not be updated anymore as their items are transfered to the SRS_TCCS - Part 3.
The general concept is described in SPT2TS-125572 - Environment and systems for the configuration management process . **[**SPPRAMSS-1229, Text **]**

5.2 Identification of the building blocks configuration

Identifications of versions
The following principles have been defined by the WG Transversal in Logical Concept
The identification of the versions of the building block are identified by the bbcVersion attribute of the Building Block Configuration which follows SEMVER (X.Y.Z).
In addition to the bbcVersion attribute, the configurationSafetyRelevance defines if the Building Block is safety-related or not. **[**SPPRAMSS-15236, Text **]**

Versioning - Process
The process of versioning shall respect the following order:

1. Realise the impact analysis according to SPPRAMSS-1170 - Impact analysis
2. Define the Level of Significance following the SPPRAMSS-1167 - Significance process
3. Increment the numbers of the version according to SPPRAMSS-15253 - Versioning - Application of the SEMVER and SPPRAMSS-8889 - Levels of Significance

ID	SPPRAMSS-15254
Type	System Requirement

Versioning - Application of the SEMVER
The application of the SEMVER defined in https://semver.org/ shall respect the following principles to number the X.Y.Z version:

- X : MAJOR version implementing incompatible interface changes between building blocks

- Y : MINOR version implementing one or several new functionalities in a backward compatible manner
- Z : PATCH version implementing backward compatible error correction or a SPPRAMSS-14487 - Patch

ID	SPPRAMSS-15253
Type	System Requirement

Link between the Logical Concept and the Evolution Management process
To connect the Evolution Management Process with the Logical Concept, and to clearly identify both the Level of Significance and the Safety Integrity Level of each building block's evolution, the following requirements are defined. **[**SPPRAMSS-15243, Text **]**

Versioning - Level of Significance
The Building Block Configuration shall have an attribute LevelOfSignificance, that can have the following values : HIGH / MEDIUM / LOW / MINIMAL as defined in SPPRAMSS-8889 - Levels of Significance .

ID	SPPRAMSS-15237
To be derived by Team	SP Task 2 CONEMP
Type	System Requirement

Versioning - Level of Significance - Rationale
The LevelOfSignificance attribute will be used by the assessor to easily analyse all the evolutions realised with a Yearly Letter of Support.
It will also be useful for the railway undertaking / infrastructure manager to have a complete view of the level of significance of the updated software. **[**SPPRAMSS-15251, Rationale **]**

Versioning - Software Integrity Level
The Building Block Configuration shall have an attribute SoftwareIntegrityLevel, that can have the following values : BIL, SIL1, SIL2, SIL3 or SIL4 as assessed by the ISA.

ID	SPPRAMSS-15240
To be derived by Team	SP Task 2 CONEMP
Type	System Requirement

Versioning - Software Integrity Level - Rationale
The SoftwareIntegrityLevel attribute will be used by the assessor to easily analyse all the evolutions realised with a Yearly Letter of Support.
It will also be useful for the railway undertaking / infrastructure manager to have a complete view of the software integrity level of the updated software. **[**SPPRAMSS-15250, Rationale **]**

Versioning - SAFE / NONSAFE attributes
The configurationSafetyRelevance attribute shall be linked to the SoftwareIntegrityLevel attribute according to the following table.

Table 20 Versioning - SAFE / NONSAFE attributes

configurationSafetyRelevance	SoftwareIntegrityLevel
NON-SAFE	BIL (non-safety-related function(s))
SAFE	

configurationSafetyRelevance	SoftwareIntegrityLevel
	BIL (safety-related function(s) with a TFFR >10-5 [h-1]) / SIL1 / SIL2 / SIL3 / SIL4

ID	SPPRAMSS-15241
To be derived by Team	SP Task 2 CONEMP
Type	System Requirement

Versioning - SAFE / NONSAFE attributes - Rationale
It is reminded that in the SPPRAMSS-8814 - [EN 50716:2023], §4.4, different processes can be applied to develop SPPRAMSS-11109 - Basic Integrity Level Software :

- implementing non-safety-related functions
- implementing safety-related function(s) with a TFFR >10-5 [h-1]

[SPPRAMSS-15252, Rationale **]**

Versioning - Linking between the X / Y / Z attributes and homologation
As defined in SPPRAMSS-8167 - Safety Assessment matrix :

- For BIL software : an evolution of the X, Y or Z number will alway lead to a yearly letter of support
- For SIL1 to SIL4 evolutions :
  - an evolution of the X number will always lead to a new certificate, because it creates an incompatibility with the other building blocks.
  - an evolution of the Y number will lead either to a letter of support or to a new certificate, depending on the SIL and the Level of Significance.
  - an evolution of the Z number will only lead to a yearly letter of support.

[SPPRAMSS-15244, Text **]**

Examples of Versioning
Example 1 :

- bbcVersion: 4.5.3
- configurationSafetyRelevance: SAFE
- SoftwareIntegrityLevel: SIL4
- levelOfSignificance : MEDIUM

Example 2 :

- bbcVersion: 1.0.3
- configurationSafetyRelevance: NONSAFE
- SoftwareIntegrityLevel: BIL
- levelOfSignificance : MINIMAL

Example 3:

- bbcVersion: 6.4.7
- configurationSafetyRelevance: SAFE
- SoftwareIntegrityLevel: BIL
- levelOfSignificance : HIGH

[SPPRAMSS-15239, Text **]**

System Identifier from TSI CCS 20223

The versioning defined in this process shall be aligned with the versioning defined in the TSI CCS 2023 as described in SPPRAMSS-7397 - 4.2.20.3. System identifier (‘system identifier’, ‘functional identifier’ and ‘realisation identifier’) **[**SPPRAMSS-15263, Issue, Open, Julien Bois **]**

6 Annex - Flowchart of the Evolution Management Process

Flowchart of the Evolution Management Process

The Evolution Management process is defined according to the following flowchart:

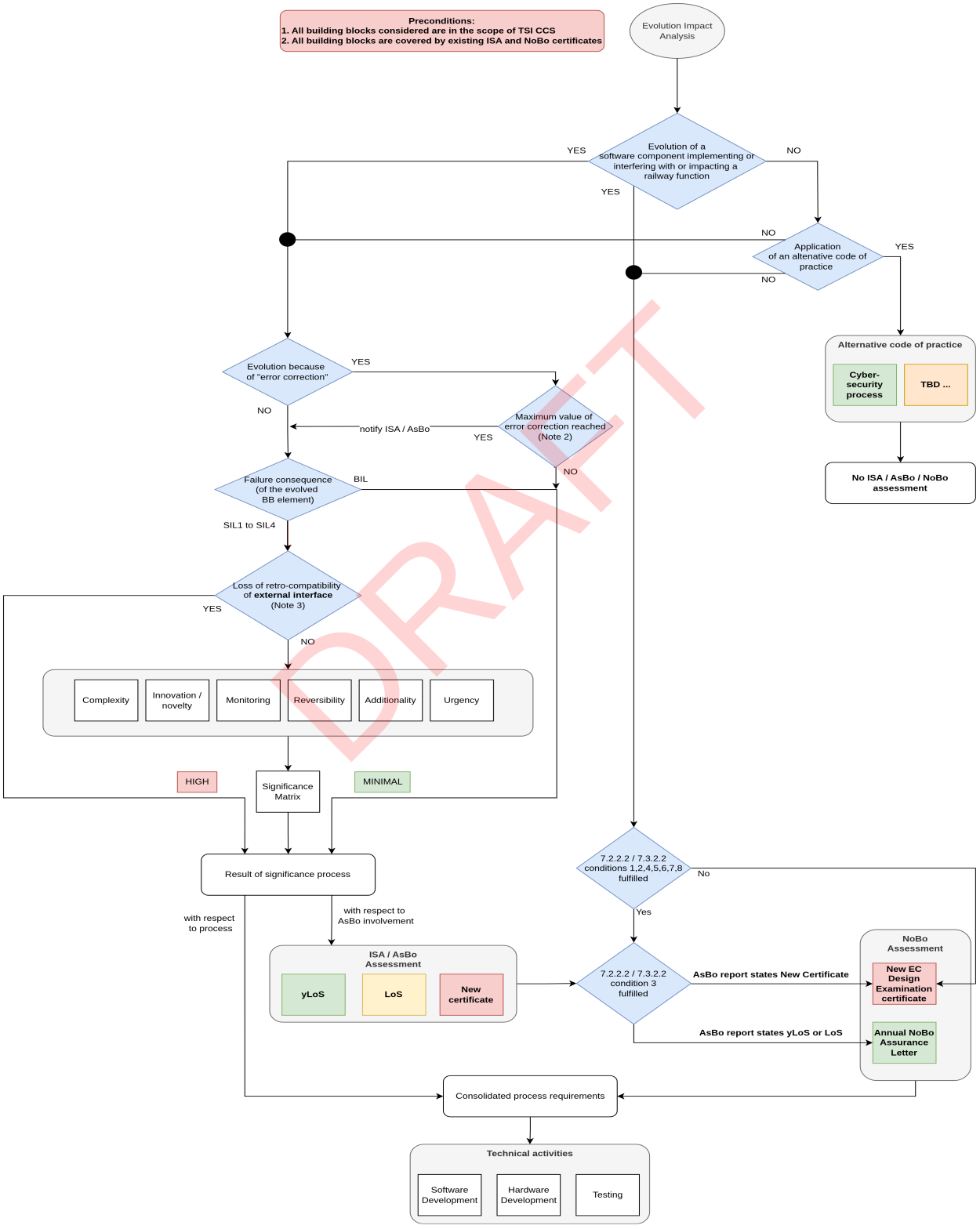


Figure 17 Evolution Management Process

Note 1:
Safety related elements can be BIL or SIL1 to SIL4. See SPPRAMSS-11109 - Basic Integrity Level for details.

Note 2:
If the answer to the specific Additionality point for "error correction" is YES/NO.
See SPPRAMSS-15259 - Rationale on Additionality in case of error correction for more context data

Note 3:
The question refers to an evolution impacting an interoperable interface at:

- physical level (e.g. mechanical, electrical)
- functional level (e.g. coding strategy

[SPPRAMSS-15980, Text **]**

7 Annex - Software complexity

Software Complexity Criteria
Complexity in this context is to be understood along the definition given in SPPRAMSS-15551 - [IEEE 610.12-1990] : "the degree to which a system or component has a design or implementation that is difficult to understand or verify" (to be clearly distinguished from the way Theoretical Computer Science uses the term, e.g. in NP-completeness, runtime complexity etc.)
This definition can be substantiated by metrics if we look at it along the concept of coherence and coupling; high coherence and low coupling mean low complexity, low coherence and high coupling mean high complexity, as immediately obvious from the following figure:

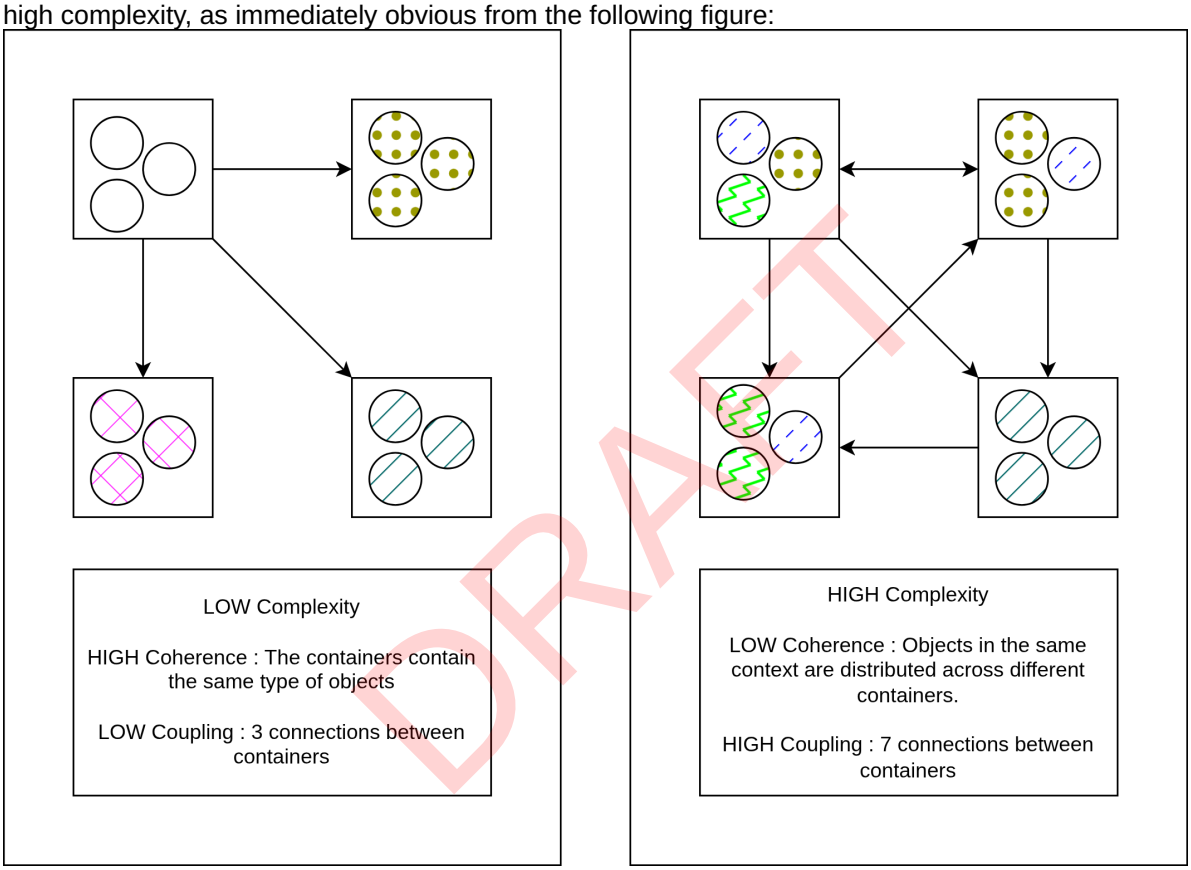


Figure 18 : illustrating coherence and coupling - coherence: same kind of objects in same container; coupling: interface relations between the containers (source: [SPPRAMSS-15552 - Softwarewartung: Grundlagen, Management und Wartungstechniken]

Software complexity shall be evaluated by the use of metrics as indicated by D.37 from SPPRAMSS-8814 - [EN 50716:2023], D.37 mentions (comments based on: SPPRAMSS-15552 - Softwarewartung: Grundlagen, Management und Wartungstechniken):

1. Graph Theoretic Complexity is a 'conventional' metric of code structure: this measure can be applied early in the lifecycle to assess trade-offs, and is based on the complexity of the program control graph, represented by its cyclomatic number; see SPPRAMSS-15553 - A complexity Measure - the cyclomatic number is based on the number of conditionals like 'if', 'for', 'while', therefore it is easy to calculate. The cyclomatic number is said to correlate well with the understandability / legibility of code. It does not cover the complexity of long individual lines of command, the recursive depth of nested loops, though, and is less helpful in object oriented programming or data-centred code.
2. number of ways to activate a certain component (accessibility): the more a component can be accessed, the more likely it is to be debugged; this metric is correlated to the effort in testing and maintenance

3. Halstead complexity measures: this measure computes the program length by counting the number of operators and operands. It provides a measure of complexity and estimates development resources; derived from the basic counts, there are a number of valuable parameters defined; let n be the number of different operators, m be the number of different operands, N be the the total number of usages of operators, M be the total number of usages of operands:
   Length ('classic' Halstead) L=N+M
   Difficulty (to read and understand) D=(n*M)/2m
   Volume V=L*$\log_2$(n+m))

   The advantage of Halstead is that it does not only count lines of code, but instead reflects complicated terms as well and is quite indifferent to the programming language. These metrics are easy to measure (simple counting) and well correlated to the frequency of programming errors. Target windows for functions is a volume V between 20 and 1000, modules should not exceed V=8000.
   Disadvantage is that Halstead does not cover the structure of code.

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

   A quick example: let's evaluate the expression

Table 21 Software Complexity Criteria

Halstead variable	parameter	detail	value
n	identified operators	subtraction addition square root square multiplication multiplication division	6
m	identified operands	a, b, c, 2, 4	5
N	total number of usage of operators	2 subtraction 1 addition 1 square root 1 square multiplication 3 multiplication 1 division	9
M	total number of usage of operands	2 a 2 b 1 c 1 2 1 4	7
L	length	N+M	16
D	difficulty	(n*M)/2m	4.2
V	volume	L*$\log_2$(n+m))	~5

4. number of entries and exits per component: minimizing the number of entry/exit points is a key feature of structured design and programming techniques. Known as well as Common Business Objectives (coupling between objects) in object oriented programming, it correlates to the frequency of programming errors in the code and reflects the testability and resusability of code, while it does not take inheritance into account.

Beyond these four examples listed in the standard, covering code volume, testability and expected residual error frequency, there are additional metrics (to e.g. cover inheritance in the object oriented case) as well as indices to indicate certain aspects of code, e.g. a maintenance index.
The maintenance index suggested by Coleman and Oman combines the metrics of lines of code,

Halstead and McCabe into one formula:
M= 171 - 5.2 * ln(average Halstead V per module) - 0.23 * (average cyclomatic complexity per module) - 16.2 * ln(average lines of code per module) + 50*sin(sqrt(2.4* average percentage of lines of comments per module))
with
M>85 indicating good maintainability
M between 65 and 85 indicating average maintainability
M<65 indicating poor maintainability
This maintenance index is well suited for strucutred programming, but less for object oriented programming.
Conclusion:
As the applicabilty and value of a metric is closely tied to the programming paradigm used, it is not possible to define one standard metric (or set of metrics) to beused for judging maintainability or changeability. Yet today, many development environments offer metrics, in particular those based on easy to perform counting operations like the ones presented here, as standard features. It is therefore to be considered mandatory that code that claims to be of a certain quality is based on coding guidelines featuring the use of metrics and defining the deduced insights and the used threshold values. Coding guidelines not covering these topics cannot be considered to reflect the current state of technology.
[SPPRAMSS-13902, Text **]**

8 Annex - Open Issues

ID	Title	Type	Status	Severity
SPPRAMSS-10153	No definition of integration activities	Issue	Open	
SPPRAMSS-13908	Competence of the organisation evolving the SuC	Issue	Open	
SPPRAMSS-13909	Re-use of widely deployed COTS	Issue	Open	
SPPRAMSS-9981	TrafficCS homologation aspects	Issue	Open	
SPPRAMSS-9693	Connection between PRAMS and IP FP2 R2DATO WP34/35 Testing	Issue	Open	
SPPRAMSS-1036	Vehicle authorisation process and trackside approval	Issue	Open	
SPPRAMSS-10240	Traceability between Common Business Objectives and System Requirements	Issue	Open	
SPPRAMSS-11467	ISA / NoBo / AsBO	Issue	Open	
SPPRAMSS-11465	Analyse that every point is handled by the process	Issue	Open	
SPPRAMSS-11523	Allignment with Train CS	Issue	Open	
SPPRAMSS-14693	IP FP2 R2DATO WP26 "T26.3. - Study on modular certification and acceptance approaches for Modular Platforms"	Issue	Open	
SPPRAMSS-13896	Linking the System Pillar Reference Architecture with the System breakdown of current European homologation process	Issue	Open	
SPPRAMSS-8884	Complexity criteria to be updated in a next revision	Issue	Open	
SPPRAMSS-8873	Hardware development process to create	Issue	Open	
SPPRAMSS-15557	Definition of the roles of the different actors	Issue	Open	
SPPRAMSS-15262	Technical Files and Patches	Issue	Open	

ID	Title	Type	Status	Severity
SPPRAMSS-15263	System Identifier from TSI CCS 20223	Issue	Open	
SPPRAMSS-15671	Assessment at integrated levels	Issue	Open	
SPPRAMSS-1001	Limitation of scope for the first and second version	Issue	Open	
SPPRAMSS-13906	Input for STIP	Issue	Open	
SPPRAMSS-14400	STIP - Yearly Letter of Support	Issue	Open	
SPPRAMSS-15347	IEC CDV 63452 - Railway applications – Cybersecurity	Issue	Open	

22 items found