# Safety Case - Strategy for Generic Design Safety Cases

| | |
|---|---|
| Author(s) | Julien Bois , Markus Spindler (Rail Expert Consult) , Iñigo Iruretagoyena Tormo , Ryf Urs (I-NAT-GST-CCS-EXT - Extern) , BUYUKAKINCAK Emre , Philipp Nienheysen , DE NICOLA, Giuseppe |
| Abstract | Second version of the document dealing with the definition of a Design Safety Case structure |
| Config Item | Safety Case |
| Document ID | Phase_5/Safety_Case-Strategy_for_GDSC#787857 Safety Case - Strategy for Generic Design Safety Cases |
| Classification | Public |
| Status | In Review by System Pillar |
| Version | 1.1 |
| Revision | 787857 |
| Last Change Date | 17.12.2025 |
| Copyright | Brussels: Europe's Rail Joint Undertaking, 2025 |



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

Review description

| | |
|---|---|
| Comments | |
| Approvals | Ryf Urs (I-NAT-GST-CCS-EXT - Extern) : Approved , BUYUKAKINCAK Emre : Approved , Philipp Nienheysen : Approved , Ramin Hedayati : Waiting , Markus Spindler (Rail Expert Consult) : Waiting , Iñigo Iruretagoyena Tormo : Approved , DE SIMONE, Vincenzo : Waiting , Morman Bettina (I-NAT-GST-CCS) : Waiting , Nicolas Ykman : Waiting , GILLIG Vincent (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - EQS1) : Waiting , ANTOONS Gilles : Waiting , DE NICOLA, Giuseppe : Approved |
| Type of Approval | Document Review |
| Attachments | |

Approval description

| | |
|---|---|
| Comments | |
| Approvals | Julien Bois : Approved , DE NICOLA, Giuseppe : Approved , CIUCCI Paolo : Waiting , Matthias Moritz : Waiting |
| Type of Approval | Document Approval |
| Attachments | |

## Table of contents

## Table of figures



## Table of tables

# 1 Preamble

## 1.1 Purpose

**Purpose of the document**

This Strategy defines how a Generic Design Safety Case structures early-phase safety evidence (Phases 1 to 5) in line with SPPRAMSS-349 - [EN 50126-1:2017] for the System Pillar (SP). It consolidates harmonised functions, interfaces, and PRAMS/testing requirements into a reusable safety argument that reduces duplication in later GPSC/GASC/SASC activities. It is developed for the scope described in PRAMS Plan. **[**SPPRAMSS-15805, Text **]**

**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 **]**

## 1.2 Intended audience

**Generic Design Safety Case Intended Audience**

This document is intended for the following users:

- Engineering Environment Team (to ensure harmonisation of content compared to the SPPRAMSS-4179 - [ERJU - SEMP]),
- System Pillar task 1 to task 4 domains,
- Innovation Pillar teams ,
- PRAMS engineers part of mirror group(s),

In addition, this document can be shared with a wider audience for informal opinion reviews:

- PRAMS engineers outside ERJU,
- 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-15796, Text **]**

### 1.3 Document context

**Context of the Generic Design Safety Case**

The GDSC complements, not replaces, GPSC and GASC. It provides harmonised baseline content that shall be referenced—not redefined—by product/application safety cases. ERJU Innovation Pillar deliverables remain governed by their processes; this document focuses on SP scope up to System Level 5 as given in SPPRAMSS-4179 - [ERJU - SEMP] **[**SPPRAMSS-15804, Text **]**

### 1.4 Glossary

#### 1.4.1 Abbreviations

**AsBo - Assessment 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-11103, 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, Definition **]**

**CBO - Common Business Objective**

Common Business Objective **[**SPLI-81, Definition **]**

**CCM - Change Control Management**

Change Control Management **[**SPLI-82, 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 **]**

**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 **]**

**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, 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 ]

**SRAC - Safety related application conditions**

This definition was merged with: SPPR-3728 - Application Condition [SPPR-2244, Definition ]

**SIL - Safety Integrity Level**

Safety Integrity Level [SPLI-1065, Definition ]

**STIP - Standardisation and TSI Input Plan**

The Europe’s Rail (EU-Rail) Standardisation and TSI Input Plan (STIP) is a collection of all outputs from EU-Rail (Innovation and System Pillar) which contribute to the goal of harmonisation of the railway system. The harmonisation topics are categorised in technical domains and described by the foreseen harmonisation channel (TSI, EN standards, SP document), the time horizon as well as dependencies with existing regulations, standards, and R&I activities. [SPLI-1849, Definition ]

**SuC - System under Consideration**

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

Traffic Management System

**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 ]

### 1.4.2 Definitions

**[Abbreviation] - 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 ]

**[Abbreviation] - 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 ]

**[Abbreviation] - Generic Design Safety Case**

The Generic Design Safety Case gives evidence to the design for a generic product or application done in Phase 1 to 5. The Generic Design Safety Case:

- fulfils the requirements of Phase 4 (including validation report) and is integrated in a modular architecture in Phase 5 of SPPRAMSS-349 - [EN 50126-1:2017],
- defines the SuC and its interfaces and must comply thereby to a harmonised reference architecture (e.g. "System Pillar Reference Architecture") with its,
  - functional allocation,
  - interfaces description,
  - standardised tests activities (e.f. test benches, procedures etc.),
  - internal and exported PRAMS requirements allocation to system functions and building blocks
- is conceived as the first argument to be presented to the ISA,
- is to be reused for further generic product safety cases or generic/specific application safety cases,
- evolves along the whole lifecycle of the SuC design,
- covers the Safety Management topics in the EU-Rail Standardisation and TSI Input Plan (STIP)

**[**SPPRAMSS-11440, Definition **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- Functional Adapter**

If legacy systems need to be integrated into a CCS system, this is expected to be realised by means of functional adapters. These adapters shall provide the harmonised functions and interfaces as far as possible:

- in the best case, the adapter is just needed for protocol conversion at the interface
- if functions are missing in the legacy product and can be implemented in the adapter at reasonable effort, they shall be implemented in the adapter
- if deviations to the harmonised functions and/or harmonised interfaces occur, this needs to be documented adequately

see SPPRAMSS-15920 - Use of functional adapters and their definitions
**[**SPPRAMSS-15996, Definition **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- SASC**

Specific Application Safety Case; SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] ,SPPRAMSS-335 - [EN 50126-2:2017] **[**SPPRAMSS-4011, Definition **]**

[Abbreviation] **- 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, Definition **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- 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 **]**

[Abbreviation] **- 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 **]**

Add a section for "SRAC/Requirement" definition => SPPRAMSS-15899 - Use of functional adapters and their definitions

**Different type of requirements**
In the context of the Generic Design Safety Case, different type of requirements are used. They differ by their origin. The following diagram aims at identifying them:

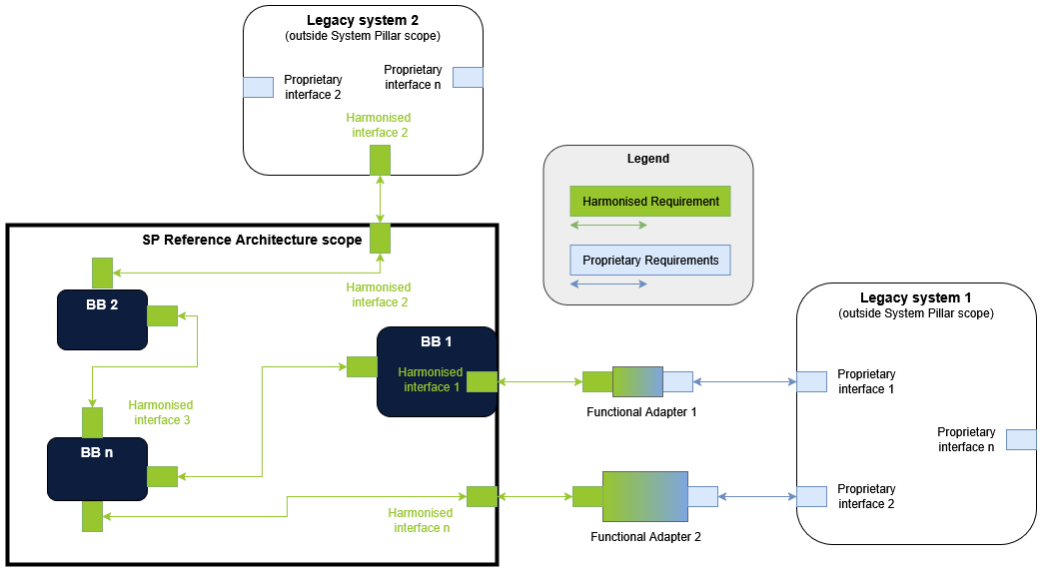


*Figure 1 Different requirements types*

- **Harmonised interfaces** are defined by the SP domains (e.g. TACS, CONEMP), and their adoption by the Building Blocks of the SP Reference Architecture (i.e. Building Blocks) is mandatory to ensure railway interoperability and system exchangeability. These interfaces are defined through **Harmonised Requirements.**
- **Proprietary interfaces** are associated with supplier-specific solutions implemented on generic products. To enable the integration of future modular Building Blocks into railway projects, solutions must be defined to connect them to legacy systems that are not part of SP. To achieve this, **Functional Adapters** are defined. The left part (i.e. green on the picture) is specified by the SP domains through **Harmonised Requirements**. The right part of the Functional Adapters (i.e. blue on the picture) shall be product-specific and defined by each supplier of the legacy system intended to be connected to the SP Building Blocks of the Reference Architecture.

  Note 1: the strategy to define either one Functional Adapter product (i.e. hardware and software) per interface or to group several interfaces into an SP gateway (i.e. multiple Functional Adapters sharing hardware and/or software resources) is left to each supplier. SP focuses exclusively on functions and interfaces needs.
  Note 2: some of the harmonised interfaces are based on existing solutions available today and therefore, no Functional Adapter applies (e.g. timing service used by Cybersecurity, some objects considered by TACS).

**[**SPPRAMSS-16242, Text **]**

## 2 References

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

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

**[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. **[**SPPRAMSS-336, Reference **]**

**[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 **[**SPPRAMSS-634, Reference **]**

**[EN 50716:2023]**

Railways Applications - Requirements for software development **[**SPPRAMSS-8814, Reference **]**

**[EN 50129:2018/AC:2019-04]**

Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling **[** SPPRAMSS-334, Reference **]**

**[EN 50155:2021]**

Railway applications – Rolling stock – Electronic equipment **[**SPPRAMSS-332, Reference **]**

**[EN 50159:2010/A1:2020]**

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems **[**SPPRAMSS-333, Reference **]**

**[EN 61703:2016]**

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

**[EN 17023: 2018]**

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

**[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
**[**SPPRAMSS-619, Reference **]**

**[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 **[**SPPRAMSS-4525, Reference **]**

**[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) **[**SPPRAMSS-328, Reference **]**

**[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 **[**SPPRAMSS-9983, Reference **]**

# 3 Business incentives for Generic Design Safety Cases

**Situation in current railway projects**

- The railway sector is working bottom-up which means from generic product or generic application to specific application (same strategy defined in SPPRAMSS-334 - [EN 50129:2018/AC:2019-04]) without harmonised reference architecture.
- The integration steps of the individual generic products and/or applications provided by different suppliers are performed by the RU/IM without harmonised procedures. As a result, every new overall integrated system leads to a new specific application preventing potential reuses for the RU/IM and progress along consolidating results.
- The bottom-up approach (i.e. GPSC to SASC) without standardised architecture bring the suppliers to define generic products and/or applications which are completely configurable but also completely different between two manufacturers.
  This generates a large number of SRAC/AC items that the integrators and RU/IM must handle, but which are not linked back to their emitters (i.e., suppliers). This is used to lead to inconsistencies and to an important time effort to perform their analysis.

**[**SPPRAMSS-11311, Text **]**

**Benefits of a Generic Design Safety Case structure**

- Thanks to a harmonised reference architecture, the overall number of (SR)AC will drastically decrease because they can be anticipated and assigned to the relevant building blocks as requirements during their development phase (i.e. until Phase 5 of SPPRAMSS-349 - [EN 50126-1:2017]),
- It is possible to realise a preliminary assessment on this harmonised reference architecture (e.g. for a top level project or for an intermediate integrated system [e.g. CCS-OB]) in phase 5 according to SPPRAMSS-349 - [EN 50126-1:2017],
- The Generic Design Safety Case also helps at limiting the risks in phase 9 during the realisation of the final safety case, validation and assessment reports,
- The evolution of element(s) part of the harmonised reference architecture (e.g. building blocks evolution) is eased as all interactions between building blocks are standardised. Impact analyses are faster and simpler and application of the *SPPRAMS/Evolution Mngt Process/Evolution_Management_in_a_Modular_Architecture* can be very efficient to improve the total cost of ownership.

**[**SPPRAMSS-11312, Text **]**

**Limitation of current version**

This preliminary version is limited to the agreement of the PRAMS team regarding the need to define a Generic Design Safety Case strategy and a first overview on how it can be represented.
From SC2.4, the PRAMS will develop these topics, define a strategy for (SR)AC management and connect this Generic Design Safety Case structure to the harmonised reference architecture defined by SP. **[**SPPRAMSS-11313, Issue **]**

# 4 Preparation of Generic Design Safety Cases

## 4.1 Introduction

### Introduction

The following sections define a process to prepare the safety case, considering the hierarchy between system safety activities and documentation. **[**SPPRAMSS-16017, Text **]**

### Scope

All provided documentation will cover only phases 1 to 5 according to the scope of this plan but might contain some input for further phases. **[**SPPRAMSS-16018, Text **]**

## 4.2 Analysis of current Safety Case structure

### Current Safety Cases

In current railway system projects, safety cases are built up from the Generic Products that are used in one or more Generic Applications that are integrated into a specific application. **[**SPPRAMSS-16022, Text **]**

### Classical safety acceptance process

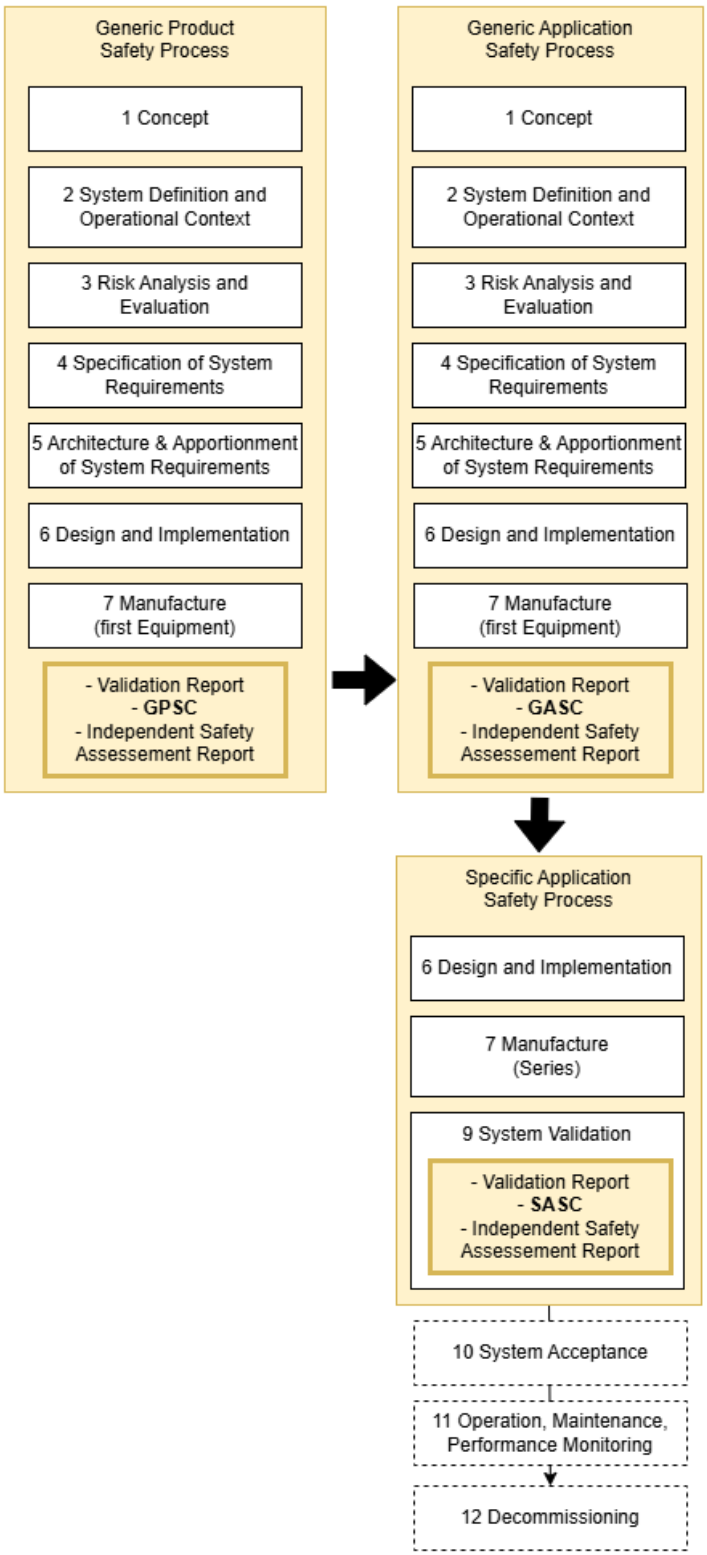


*Figure 2 Example of classic safety acceptance processes (Source EN 50126-2:2017 Fig. 3)*

[SPPRAMSS-16020, Diagram ]

**Issues of contemporary Safety Case Hierarchy**

The currently used safety case structure has the following issues that lead to increased efforts for integration, assessment,

certification and change management:

1. The possibility to reuse a SASC in future projects is very limited.
2. As the application is unknown on product safety case level, lots of SRACs will be posed that have to cover various possible application scenarios.
3. Integration efforts are high, as the SASC has to show that the combination of the chosen generic applications result in a safe system.
4. SASC as the only system level safety case often identifies hazards resulting from the combination of generic products and applications that lead to changes in the applications in late project phases.
5. The allowed configurations (combinations of different versions of generic applications and products) is only defined in the specific application safety case.
6. A change on lower levels leads to a flood of document changes on upper levels, even if the impact is well contained in the product or generic application.
7. In today's safety case structures, the safety cases are mainly aggregated bottom-up. This results in a complicated SRAC management which directly contributes to the complexity of the SASC.

Majority of these issues can be mitigated by choosing a combined top-down & bottom-up approach including the GDSC. This is illustrated on SPPRAMSS-16024 - Example of actual and targeted structure for modular safety cases. [SPPRAMSS-16021, Issue ]

**Example of actual and targeted structure for modular safety cases**

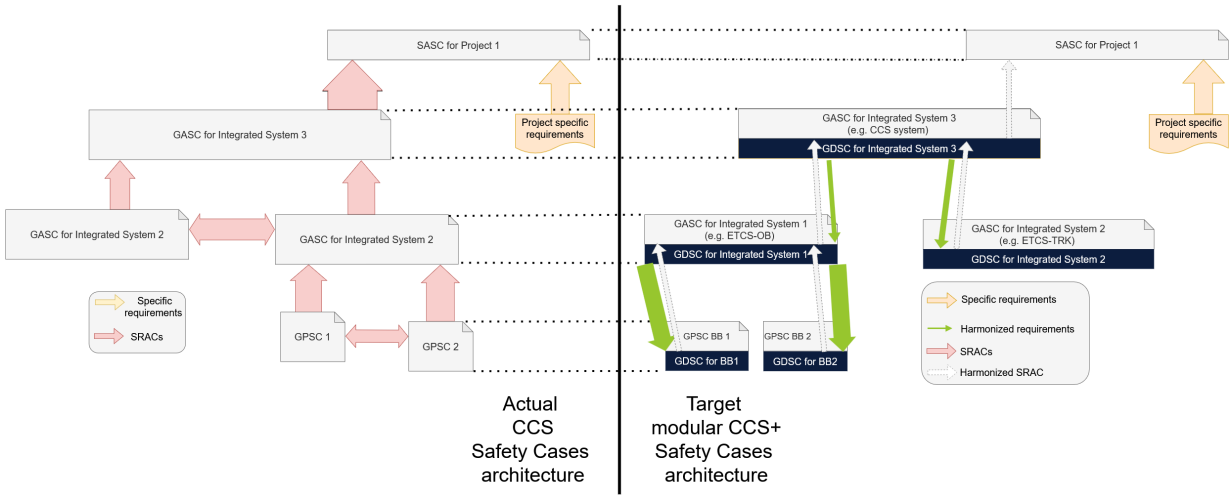


*Figure 3 Actual and targeted safety architectures*

For definitions for each requirement see SPPRAMSS-16242 - Different type of requirements .

[SPPRAMSS-16024, Diagram ]

**Details on example of actual and targeted structure for modular safety cases**

Actual and targeted structure of modular safety cases are given in SPPRAMSS-16024 - Example of actual and targeted structure for modular safety cases. Actual Safety Case Structure (Current Approach) diverging in its,

- Bottom-up aggregation:
  - Safety cases start at the Generic Product Safety Case level.
  - These feed into Generic Application Safety Cases and finally into the Specific Application Safety Case.
- SRAC Explosion:
  - Arrows between GPSCs represent Safety-Related Application Conditions required for interaction.

    - The number of SRACs grows exponentially at higher levels, creating complexity.
- Project-specific requirements:
    - Each project introduces unique requirements linked to equipment configuration, feeding into the SASC.
- Full workload at project level:
    - Most safety case activities are repeated for each project, increasing cost and time.

On the other hand, based on SP Reference Architecture, Targeted Modular Architecture (Ideal Approach) grants,

- Harmonized requirements:
    - Requirements for interfaces, functions, PRAMS and testing are provided upfront.
- Integrated SRACs:
    - Most SRACs between building blocks (BBs) are already addressed in harmonised requirements.
    - Harmonized SRACs refer to generic SRACs coming from the reference architecture to systems or stakeholders which are outside SP scope. The technical/safety need is common for a Building Block defined by the reference architecture (provided by any supplier), however, its implementation by a non-standardised system/procedure outside SP scope will differ.
- Shared workload:
    - GDSC activities (Phases 1–5 per EN 50126) handled by System Pillar.
    - Integration activities (Phases 5–11) handled by suppliers/integrators with the support of the PRAMS team for Phase 11 with Evolution Management process
- Reduced complexity:
    - Remaining SRACs are harmonised as far as possible.
    - Project-specific requirements only feed into the SASC minimally

**[**SPPRAMSS-16249, Text **]**

**Generic Design Safety Cases content**

The Generic Design Safety Case for a Building Block or an integrated system demonstrates that the PRAM and Safety Requirements (e.g. TFFRs, SILs, response time) defined by the System Pillar (SP) domains and allocated to that scope are fully addressed. All requirements necessary to ensure safe integration (e.g. between two Building Blocks exchanging safety-related data) are handled at the integrated level through harmonised requirements and are allocated to the relevant Building Blocks. Therefore, no SRAC between elements defined by the System Pillar domains is required. **[**SPPRAMSS-16041, Text **]**

### 4.3 Analysis of future Generic Design Safety Case structure

**Need to rework the acceptance process**

Following the definition of the targeted modular CCS+ safety cases architecture, there is a need to rework the actual safety acceptance process by introducing the GDSC. **[**SPPRAMSS-16104, Text **]**

**Interrelation of design and integration**

SPPRAMSS-16023 - Example of safety acceptance processes in a modular architecture shows the inter-relation of design and integration. While the classic RAMS phases look like project phases that are passed one after another, in real integration projects they run in parallel for design, manufacturing of the used projects and integration. **[**SPPRAMSS-16040, Text **]**

**Actors performing integration activities**

Integrators are typically considered to be mainly Railway Undertakings (RUs) and Infrastructure Managers (IMs), while manufacturers are viewed as the supplying industry. In practice, however, large-scale integration projects are often

awarded to suppliers, or even to consortia of suppliers, who takes full responsibility for system integration. During the operation and maintenance phases, RUs and IMs usually assume this role, acting as integrators for system modifications, upgrades, and retrofitting activities. **[**SPPRAMSS-16038, Text **]**

**Early safety argument with Generic Design Safety Case**

The Generic Design safety case fits in this realistic scenario by providing an early safety argument for the later integration (i.e. in Phase 5 of EN 50126), without having to wait on the Generic Product and Application Safety Cases. It will ease the later change and evolution processes as the PRAMS requirements are documented independent of the actual products and generic applications used in the integrated system. **[**SPPRAMSS-16039, Text **]**

**Basis of Generic Design Safety Case**

The Generic Design Safety Case is based on the PRAMS activities performed from Phase 1 to 5 analysis of EN 50126 and the validation of the requirements as requested by EN 50126-1, section 7.5.4 - *Specific validation tasks* for RAMS Phase 4. **[**SPPRAMSS-16025, Text **]**

**Example of safety acceptance processes in a modular architecture**

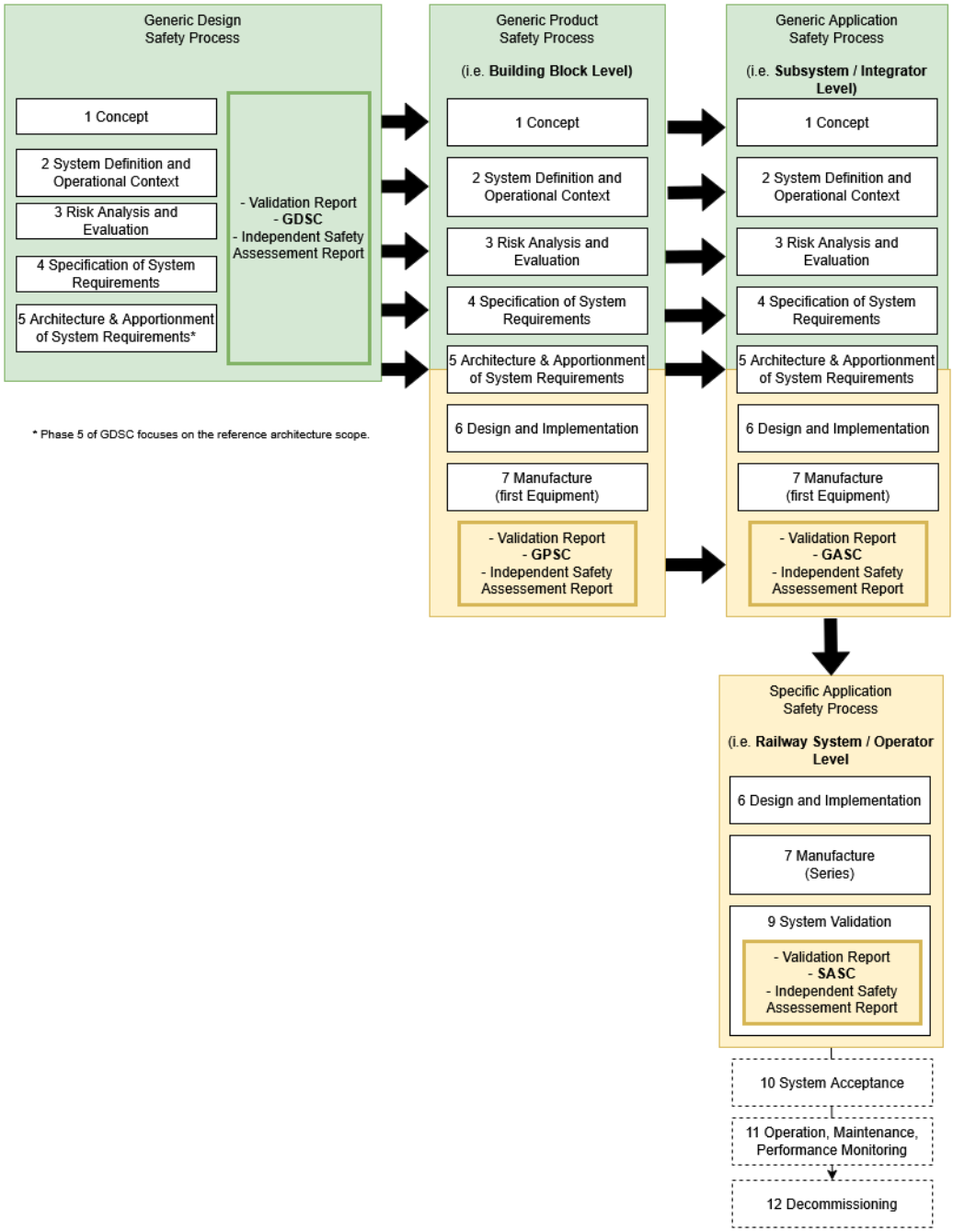


*Figure 4 Example of safety acceptance processes with GDSC*

**[**SPPRAMSS-16023, Diagram **]**

**Example of safety acceptance processes in a modular architecture - Explanations**

SPPRAMSS-16023 - Example of safety acceptance processes in a modular architecture illustrates how the introduction of the Generic Design Safety Case modifies the traditional safety acceptance process. In the classical approach, safety cases are built bottom-up from Generic Product Safety Cases (GPSC) and Generic Application Safety Cases (GASC) toward the Specific Application Safety Case (SASC). This often leads to complexity, late hazard identification, and numerous Safety-Related Application Conditions (SRACs).

With GDSC integrated:

- **Early Harmonisation**: the GDSC provides a harmonised reference architecture and predefined PRAMS requirements during RAMS Phases 1–5, reducing duplication and inconsistencies.
- **Role of GPSC/GASC**: these now focus mainly on customer-specific requirements (e.g., RU/IM needs) rather than redefining baseline safety content. The GDSC acts as a stable foundation.
- **Acceptance Process Simplification**: instead of revalidating common requirements for every project, the GDSC content is checked for coverage, not recreated. This limits branching and prevents proliferation of variant-specific safety cases.
- **Impact on Integration**: by embedding safety arguments early, the process mitigates risks in later phases (integration and homologation), reducing cost and effort.

In short, the GDSC serves as a central safety argument, enabling modularity, reuse, and streamlined acceptance. **[**SPPRAMSS-16243, Text **]**

### 4.4 Safety Cases Structure proposed for ERJU framework

**Structure of Generic Design Safety Case**

The Generic Design Safety Case structure itself shall follow the SP Reference Architecture with the various functions and interfaces it defines. This hierachical structure allows a work split of the detailed hazard analysis and requirements management activities and also a top-down approach providing an overall risk analysis, TFFR allocation and SRAC data base from SASC to GPSC (i.e. through harmonized PRAMS requirements). **[**SPPRAMSS-16044, Text **]**

**Granularity of Generic Design Safety Cases for Functions**

The granularity of the Generic Design Safety Cases shall follow the split of functional specifications as well as the foreseen SP Reference Architecture. The goal - as in every System Definition chapter of a safety case - is to find a scope that is well assessable. The current proposal from the PRAMS team regarding the granularity and hierarchy and Generic Design Safety Cases is presented in SPPRAMSS-16027 - PRAMS Team proposal of implementation of Safety Case structure in railways.

**[**SPPRAMSS-16042, Text **]**

**PRAMS Team proposal of implementation of Safety Case structure in railways**

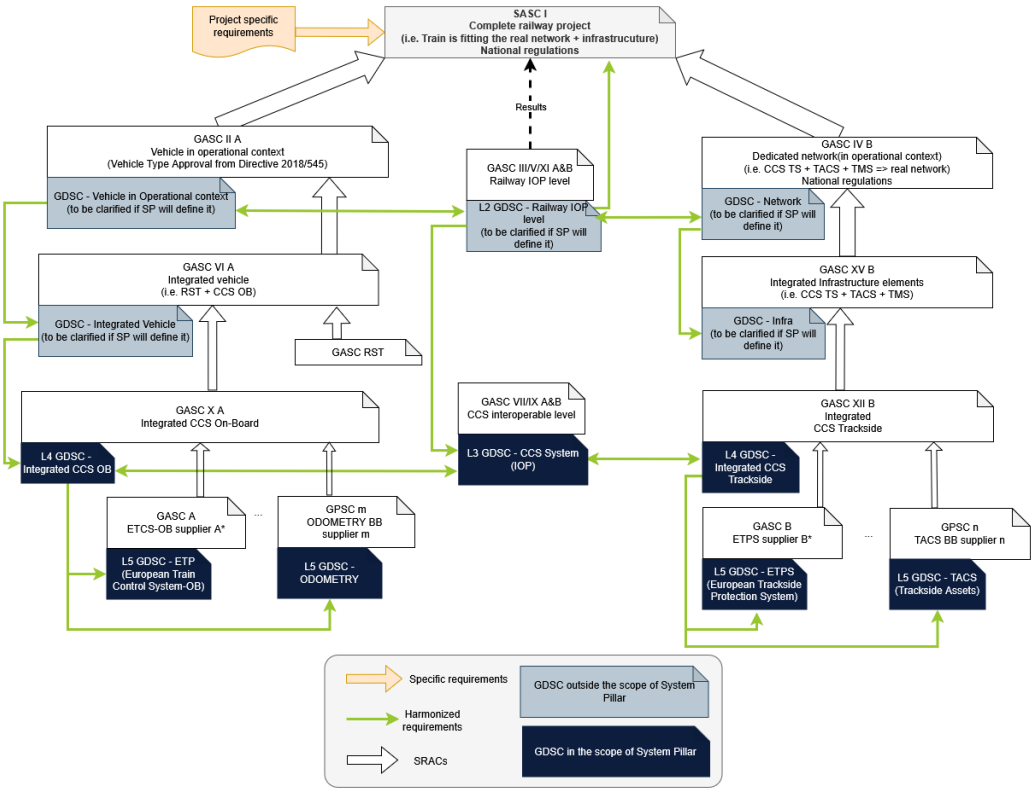


*Figure 5 Example of implementation of Safety Case structure in railways*

**[**SPPRAMSS-16027, Diagram **]**

**Notes on PRAMS Team proposal of implementation of Safety Case structure in railways**

From SPPRAMSS-16027 - PRAMS Team proposal of implementation of Safety Case structure in railways :

- The given Roman numbers are taken from the Swiss regulation SPPRAMSS-9983 - [DMS-ID SA21-00453 - Systemführerschaft ETCS CH].
- The ETCS-OB and ETPS are provided by their suppliers as GASC; meaning that they are programming the generic application (e.g. ETCS BSL4.0) on their generic product, both based on L5 GDSC ETCS-OB or ETPS.
- It is not foreseen in SP to decouple the generic application software (e.g. ETCS BSL4.0) from the generic product parts for those two building blocks (this is not an exhaustive list)
- It is intended to show the highest level of genericity for this railway system; only the final step becomes specific. In other projects, specific safety case(s) may be used at lower level, depending on the business strategy (e.g. a single fleet of vehicle is deployed by the RU)
- The levels Lx are coming from SPPRAMSS-624 - Scope of view from hierarchical process point of view
- All "Project specific requirements" coming from the customer(s) (e.g. RU/IM) should be limited as much as possible to avoid variants of a same product from suppliers to fulfil each customers needs (e.g. "comfort" requirements). This situation is faced today and it complicates the concept of "Generic Products". **No specific customer requirement can jeopardise the Generic Design Safety Case content.**

**Open questions:**

- Grey GDSC are required to get a complete modularity of railway system but are outside SP scope. How to cover them?
- What about TMS? What will be the outputs from Task 3; standardised requirements, SRACs?

- Shall we have a last GASC just before the SASC which would cover "Harmonised railway system" / "Harmonised ERTMS L2 Line"... This would drastically reduce the scope of future SASC.
- Should we differentiate the GDSC at BB level from Design SC at Application (i.e. today's covering integration activities) levels with using different naming (e.g. Generic Integration Safety Case)?

[SPPRAMSS-16246, Text ]

**Scope of view from hierarchical process point of view**

Scope of view from hierarchical process point of view.

Source: System Pillar “System of Systems (SoS)” approach - Europe's Rail (europa.eu) > https://rail-research.europa.eu/system_pillar/system-pillar-system-of-systems-sos-approach/

*Table 1 : Hierarchical Levels SP System of Systems*

| System Level | Area (example) | Level of process details, examples (indicative) |
|---|---|---|
| Level 1 | Public Transport | The basic requirements, how railways and other transport systems shall interact concerning management connections in a station. |
| Level 2 | Railway System | How shall customer care, ticket sales, customer information, TMS and CCS interact in general to manage a deviation (described as basic requirements). |
| Level 3 | CCS- Command and Control Systems | How shall different actors in the production (trains, field forces, ..) be coordinated to execute a changed plan (requirements, basic process). |
| Level 4 | Vehicle Control and Supervision<br>Trackside Control and Supervision | What processes shall happen onboard in general when the movement authorisation changes (requirement, basic process).<br>What processes shall happen in general when the moveable trackside elements changes. |
| Level 5 | Onboard Safety Logic<br>Trackside Safety Logic | What is the safety reaction to a change of the movement authorisation.<br>What is the safety reaction to a change of point position. |

[SPPRAMSS-624, Text ]

### 4.5 Migration and integration of legacy products and applications

**Use of functional adapters and their definitions**

Individual solutions are expected to define their adapters whose safety case are adapted to GDSC. To be explained in a next version. [SPPRAMSS-15899, Issue ]

**Use of functional adapters and their definitions**

The CCS Generic Design Safety Case defines the blueprint for the safety case of a CCS system implementing the CCS target reference architecture of the System Pillar.

The CCS Generic Design Safety Case is intended and expected to safely integrate the Generic Design Safety Cases of the underlying system levels, as described in SPPRAMSS-16027 - PRAMS Team proposal of implementation of Safety Case structure in railways. During the migration phase, when the target CCS reference architecture is not yet fully implemented, legacy systems need to be integrated with the Generic Design Safety Case structure in a reasonable way. The strategy to

be followed is:
As soon as a specific implementation of a CCS systems claims to aim for a migration path towards the reference architecture, the safety argument of that CCS system is required to use the Generic Design Safety Case as a basis and to document every deviation from it, together with an appropriate rationale for the necessity of the deviation. A claim for migration or even for compliance to the reference architecture shall be considered inappropriate if such information is missing or incomplete.
Legacy systems are expected to be integrated into such a CCS system by functional adapters. These adapters shall provide the harmonised functions and interfaces as far as possible:

- in the best case, the adapter is just needed for protocol conversion at the interface
- if functions are missing in the legacy product and can be implemented in the adapter at reasonable effort, they shall be implemented in the adapter
- if deviations to the harmonised functions and/or harmonised interfaces occur:
  - every deviation shall be documented
  - there shall be given a rationale why the deviation is necessary
  - there shall be given a strategy on how and when the deviation is overcome in the migration path towards the reference architecture
- a safety case for either the adapter itself or for the integrated system of adapter and legacy system (whichever is better suited for the specific case) shall be provided, making reference to the Generic Design Safety Case(s) of the building blocks of the reference architecture which are missing because of the use of the legacy product. All aspects relevant for safe integration into the Generic Design Safety Case structure need to be pointed out and documented in adequate depth in the section 'relations to other safety cases', wherever necessary supported by means of SRAC or usage restrictions, and, from a RAMS perspective, the intended migration path towards the reference architecture shall be described in that safety case in the system definition and safety management sections.

**[**SPPRAMSS-15920, Text **]**

## 5 FAQ

**What is a Generic Design Safety Case, in short?**

It is a baseline of documentation developed in the System Pillar, providing evidence that the design for a generic product or application (Phases 1–5) is safe. It defines the system under consideration (SuC), its interfaces, and complies with a harmonised reference architecture. It serves as the first safety argument for the Independent Safety Assessor (ISA) and is reused for later safety cases.
**[**SPPRAMSS-14711, Text **]**

**Why do we need a Generic Design Safety Case?**

To avoid dissipation of responsibility and collect evidence demonstrating that the System Pillar design is safe. It also reduces complexity, enables reuse, and mitigates risks during later integration phases.
**[**SPPRAMSS-14706, Text **]**

**When do we create a Generic Design safety case?**

When the System Pillar design is frozen, typically by the end of RAMS Phase 5.
**[**SPPRAMSS-14699, Text **]**

**What is the content going to be?**

A subset of requirements necessary for the harmonised railway system, following SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] structure and Traceability Matrix. It includes safety arguments, risk analysis, and allocation of PRAMS requirements to functions and building blocks.
[SPPRAMSS-14709, Text ]

**What is not going to be in the content?**

- Documentation related to phases not covered by System Pillar activities (beyond Phase 5).
- Any functionality not harmonised by the System Pillar.

[SPPRAMSS-14710, Text ]

**Who creates the Generic Design Safety Case?**

System Pillar domains responsible for corresponding functions, in collaboration with the PRAMS team.
[SPPRAMSS-14707, Text ]

**What input is needed to create a Generic Design safety case?**

- Function definitions
- Interface definitions
- System architecture
- Risk analysis
- Documentation from SPPRAMSS-349 - [EN 50126-1:2017] for Phases 1–5
- All documentation generated by System Pillar.

[SPPRAMSS-14703, Text ]

**What architecture will it be based on?**

The System Pillar reference architecture, which defines the system breakdown of the railway system.
[SPPRAMSS-14708, Text ]

**Does the scope include RAM topics?**

Yes, to break down safety targets according to SPPRAMSS-334 - [EN 50129:2018/AC:2019-04].
[SPPRAMSS-14705, Text ]

**Which kind of RAM info/input is needed?**

RAM data supporting risk analysis and allocation of reliability, availability, and maintainability targets to system functions and building blocks.
[SPPRAMSS-14704, Text ]

**Is this the same than a Modular Safety case?**

No. A Modular Safety Case is about the overall structure combining all safety cases needed for operation. Generic Design Safety Case is an early-phase baseline that can feed into modular safety cases.
[SPPRAMSS-14700, Text ]

**How is the Generic Design Safety Case related to Generic Product and Generic Application Safety case?**

It serves as an input and baseline for GPSC and GASC, covering early phases and harmonised requirements.
**[**SPPRAMSS-14701, Text **]**

**Do we need to update the PRAMS plan with respect to the Generic Design Safety case?**

Yes, the PRAMS plan must reflect the strategy and evolution management for Generic Design Safety Case activities.
**[**SPPRAMSS-14702, Text **]**

**How can the Generic Design Safety Case evolve in future?**

It will grow along the lifecycle, integrate migration strategies for legacy systems, and adapt to changes in harmonised architecture and PRAMS requirements. It may also include functional adapters for legacy integration.
**[**SPPRAMSS-14713, Text **]**

## 6 Compliance to EN 50129 and templates

**Traceability with EN 50129 and template**

The PRAMS team will provide in a next version an exhaustive traceability of every section of the Safety Case structure (i.e. section 7 - *The Safety Case: structure and content* from SPPRAMSS-334 - [EN 50129:2018/AC:2019-04] for each Generic Design Safety Case used in SP Reference Architecture.
The template is already avaialble (PRAMS - Generic Design Safety Case - Template) but not yet fitted to each level of Generic Design Safety Case. **[**SPPRAMSS-16255, Issue **]**