


Generic Design Safety Case - Strategy

Author(s)	Bois Julien (I-NAT-GST-CCS-EXT - Extern) , Markus Spindler (Rail Expert Consult) , Iñigo Iruretagoyena Tormo , LARBAT Guy-EXT , Ryf Urs (I-NAT-GST-CCS-EXT - Extern)
Abstract	Second version of the document dealing with the definition of a Design Safety Case structure
Config Item	
Document ID	Phase_5/GDSC-Strategy#596662  Generic Design Safety Case - Strategy
Classification	Public
Status	Open
Version	1.1
Revision	596662
Last Change Date	28.05.2025

Copyright

Brussels: Europe's Rail Joint Undertaking, 2025

© Europe's Rail Joint Undertaking, 2025

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorizes you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following mention [EU Rail trade mark, title of the document, year of publication, version of document, URL].

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in the this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trade marks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

INFO: History table is not displayed, because this document is in status **doc_open**.

RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }

CONTACT: For more information contact Administrator

1 Table of contents

1	Table of contents	3
2	Table of figures	4
3	References	5
3.1	Documentation	5
3.2	Abbreviations	6
3.3	Definitions	9
4	Business incentives to realise a Design Safety Case	12
5	Process to prepare the Safety Case	13
5.1	Introduction	13
5.2	Analysis of current safety case structure	13
5.3	Safety Case Structure proposed for ERJU framework	15
5.4	Design Safety Case within RAMS Phases	18
5.5	Safety Case Structure for migration and integration of legacy products and applications	20
5.6	Composition of the Design Safety Case	20
6	Compliance to EN 50129	21

2 Table of figures

Figure 1 Classical Safety Case Structure

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

Figure 3 Example of safety acceptance processes with GDSC

Figure 4 Example of Safety Case Structure for Modular Design

Figure 5 Generic Design Safety Case (GDSC) in the Context of RAMS Phases

Figure 6 Safety Case Structure with Design Safety Case for migration and legacy subsystems

Figure 7 Design Safety Case Structure

3 References

3.1 Documentation

[EN 50126-1:2017]



Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[EN 50126-2:2017]

Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[EN 50128:2011 + A2/2020]

Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems

Nota: The standard is superseded by  SPPRAMSS-8814 - [EN 50716:2023], but the  SPPRAMSS-328 - [TSI CCS + (EU) 2023/1695] does not mention yet the standard.

[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

[EN 50716:2023]

Railways Applications - Requirements for software development

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

Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[EN 50155:2021]

Railway applications – Rolling stock – Electronic equipment

[EN 50159:2010/A1:2020]

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[EN 61703:2016]

Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[EN 17023: 2018]

Railway applications - Railway vehicle maintenance - Creation and modification of maintenance plan

[CSM RA + (EU) No 1136/2015]

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

[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

[TSI CCS + (EU) 2023/1695]

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)

3.2 Abbreviations

SPLI-219, [Abbreviation] - 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

SPPRAMSS-11109, 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.

SPLI-81, CBO - Common Business Objective

Common Business Objective


SPLI-82, CCM - Change Control Management

Change Control Management

SPPRAMSS-11099, CCS - Control-Command and Signalling

Control-Command and Signalling

SPPRAMSS-10184, 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-11100, 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-343, CSM-RA - Common safety method for Risk evaluation and Assessment

'common safety method for Risk evaluation and Assessment' means the methods describing the assessment of safety levels and achievement of safety targets and compliance with other safety

requirements;  SPPRAMSS-619 - [\[CSM RA + \(EU\) No 1136/2015\]](#)

SPLI-93, DAC - Digital Automated Coupling

Digital Automated Coupling

SPPRAMSS-11101, 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-11117, ERP - Enterprise Ressource Management

Enterprise Ressource Management

SPPRAMSS-8881, GASC - Generic Application Safety Case

Generic Application Safety Case (from  SPPRAMSS-334 - [\[EN 50129:2018/AC:2019-04\]](#))


SPPRAMSS-8880, GPSC - Generic Product Safety Case

Generic Product Safety Case (from  SPPRAMSS-334 - [\[EN 50129:2018/AC:2019-04\]](#))

SPPRAMSS-11112, 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-11104, ISA - Independent Safety Assessor

The role is defined in "Table G.4 — Role specification for Independent Safety Assessor" of  SPPRAMS S-335 - [\[EN 50126-2:2017\]](#)

SPPRAMSS-11116, LoS - Letter of Support

Letter of Support

SPPRAMSS-11114, LRU - Line Replaceable Unit

Line Replaceable Unit

SPPRAMSS-11113, SRU - Shop Replaceable Unit

Shop Replaceable Unit

SPPRAMSS-11107, 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-11105, 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](#).

SPPRAMSS-11102, 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-4011, [Abbreviation] - SASC

Specific Application Safety Case;  SPPRAMSS-334 - [\[EN 50129:2018/AC:2019-04\]](#) , 
SPPRAMSS-335 - [\[EN 50126-2:2017\]](#)

SPPR-2244, SRAC - Safety related application conditions

This definition was merged with:  SPPR-3728 - [Application Condition](#)

SPLI-1065, SIL - Safety Integrity Level

Safety Integrity Level

SPLI-1849, 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.

SPPRAMSS-8882, SuC - System under Consideration

System under Consideration (from  SPPRAMSS-334 - [\[EN 50129:2018/AC:2019-04\]](#))

Traffic Management System

SPPRAMSS-11110, TCMS - Train Control and Monitoring System

Train Control and Monitoring System

SPPRAMSS-11115, yLoS - Yearly Letter of Support

Yearly Letter of Support

3.3 Definitions

SPT2ARC-940, [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-939, [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-808, [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.

SPPRAMSS-11440, [Abbreviation] - Design Safety Case

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

- fulfil the requirements of Phase 4 (including validation report) and integrated in a modular architecture in Phase 5,
- define the SuC and its interfaces and must comply thereby to a harmonised reference architecture (e.g. "System Pillar Reference Architecture"):
 - functional allocation,
 - interfaces description,
 - standardised tests activities (e.f. test benches, procedures),
 - allocation of safety requirements (e.g. TFFR, SRAC)
- be presented to the ISA for a first statement,
- be reused for further generic product safety cases or generic/specific safety cases,
- evolve along the whole lifecycle of the SuC design,
- cover the Safety Management topics in the EU-Rail Standardisation and TSI Input Plan (STIP).

SPPRAMSS-9973, [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 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.

SPLI-1031, [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.

SPT2ARC-1011, [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-1013, [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-1286, [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-937, [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-936, [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.





4 Business incentives to realise a Design Safety Case

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 results in an large number of SRAC/AC to be handled by the integrators and RU/IM which are not looped with their emitters (i.e. suppliers). This use to lead to inconsistencies and to an important time effort to perform their analysis.

[SPPRAMSS-11311]

Benefits of a 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 **Design Safety Case** also helps at limiting the risks in phase 9 during the realisation of the final safety case, validation and assessment reports as most of "paper" work has been realised and checked during phase 5 according to  SPPRAMSS-349 - [EN 50126-1:2017],
- 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  **Evolution management of safety-related modular systems - Process and organisation** can be very efficient to improve the total cost of ownership.

[SPPRAMSS-11312]

Limitation of current version

This preliminary version is limited to the agreement of the PRAMS team regarding the need to define a **D**

esign 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 Design Safety Case structure to the harmonised reference architecture defined by SP.

5 Process to prepare the Safety Case

5.1 Introduction

The following sections define a process to prepare the safety case, considering...

The following sections define a process to prepare the safety case, considering the hierarchy between system safety activities and documentation. [SPPRAMSS-1360]

All provided documentation will cover only phases 1 to 5 according to the 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-1359]

5.2 Analysis of current safety case structure

Figure # Classical Safety Case Structure

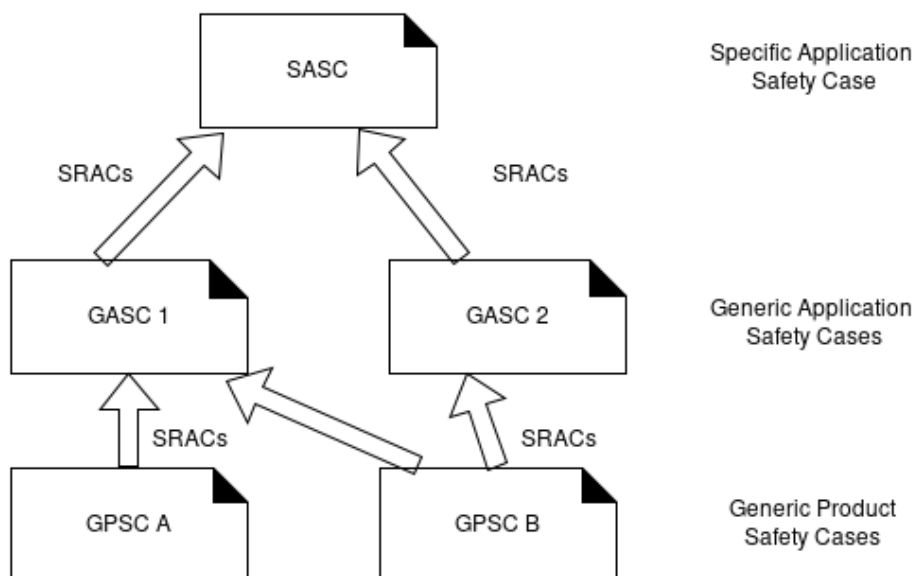
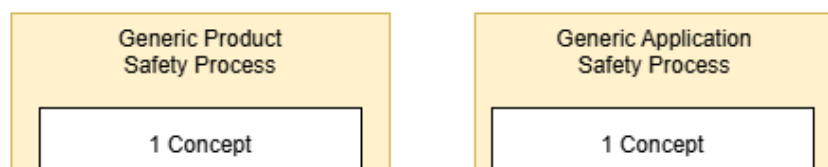


Figure 1 Classical Safety Case Structure

Classical safety acceptance process



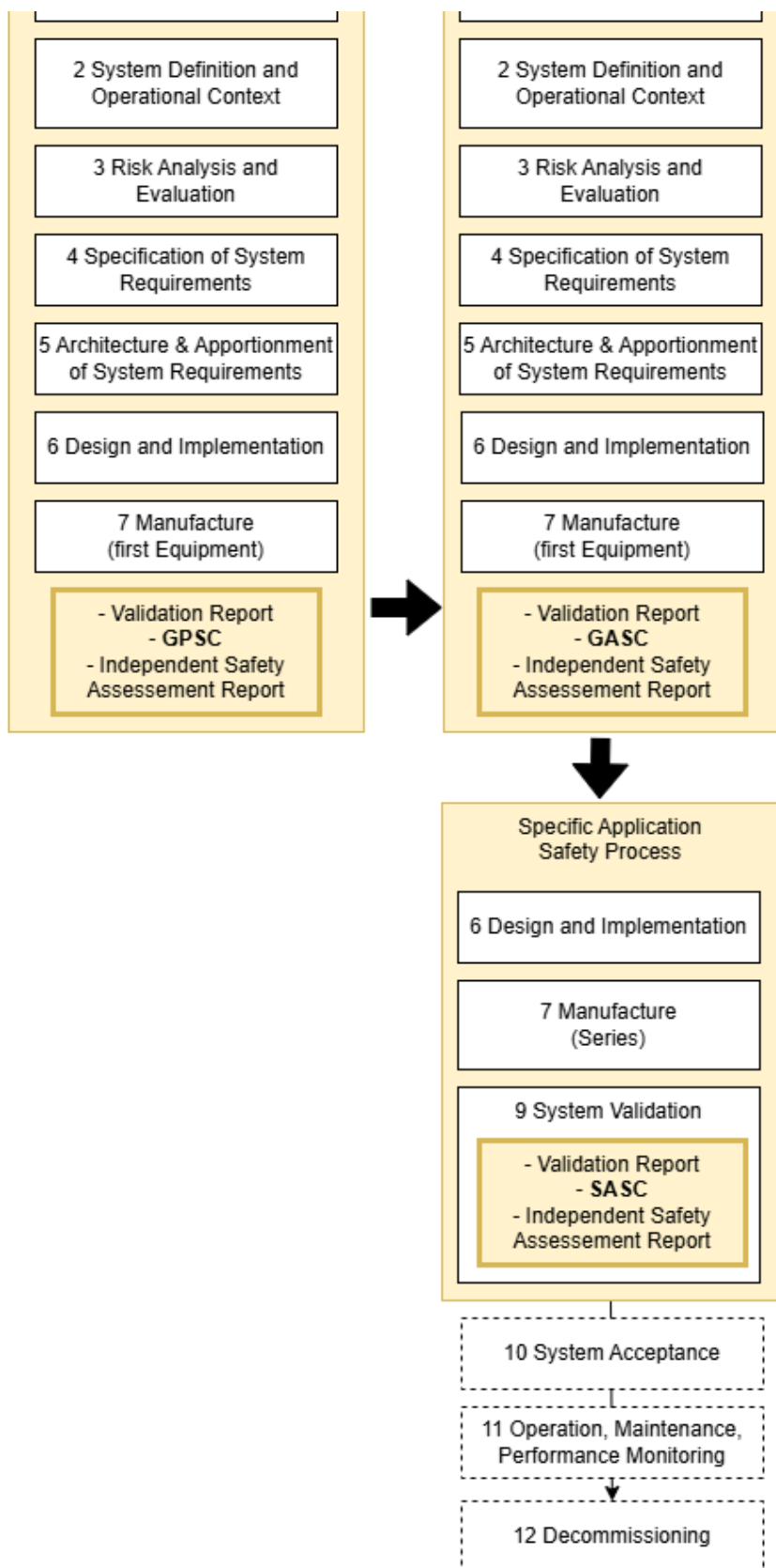


Figure 2 Example of classic safety acceptance processes (Source EN 50126-2:2017 Fig. 3)

In current railway system projects, safety cases are built up from the Generic P...

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-418]

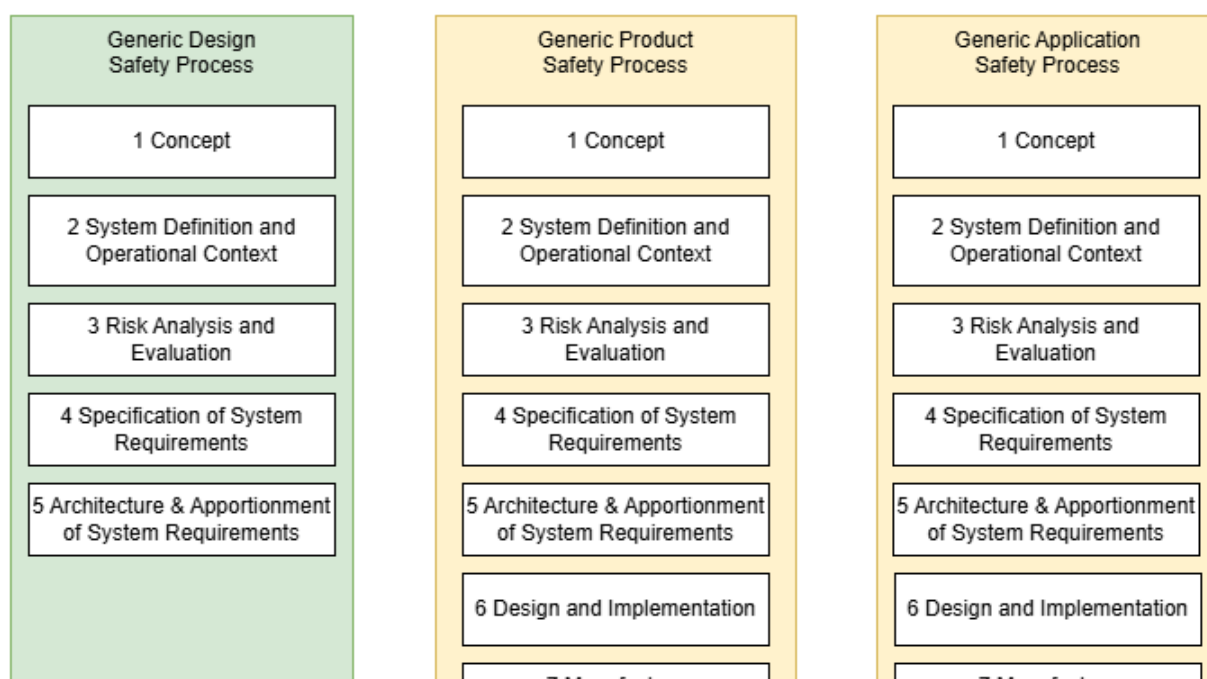
Issues of contemporary Safety Case Hierarchy

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.

5.3 Safety Case Structure proposed for ERJU framework

Example of safety acceptance processes in Modular Design



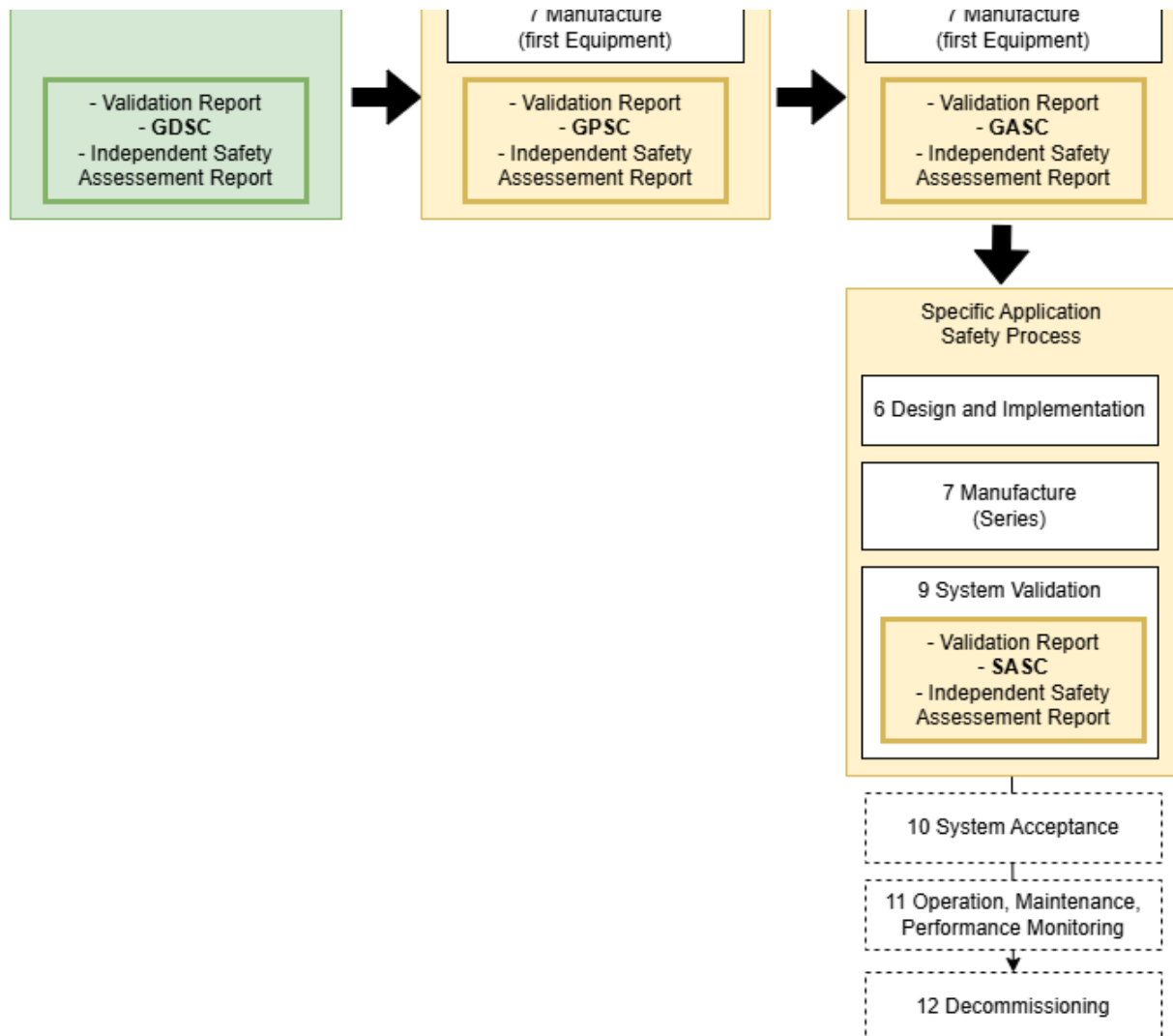


Figure 3 Example of safety acceptance processes with GDSC

Example of Safety Case Structure for Modular Design



A Design Safety Case provided as early as RAMS Phase 5 shall show the safety of the system by providing the safety arguments under the conditions that the modules (products, generic applications) and the breakdown of the system into modules meet the safety and functional requirements presumed by the Design Safety Case. [SPPRAMSS-415]

The Design Safety Case is based on the risk analysis (RAMS Phase 3) and the validation of the requirements as requested by ☐ SPPRAMSS-349 - *Missing cross-reference*, section 7.5.4 for RAMS Phase 4 [SPPRAMSS-417]

5.4 Design Safety Case within RAMS Phases

The following Figure shows the interrelation of design and integration. While th...

The following Figure shows the interrelation 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-2946]

We can think of the integrators to be mainly the RUs and IMs, while manufacturer...

We can think of the integrators to be mainly the RUs and IMs, while manufacturers are the supplying industry, but in reality large integration projects are often contracted to suppliers or even consortiums of suppliers responsible for integration. During operation and maintenance however, RUs and IMs take over and often take the role of integrator for changes and retrofit. [SPPRAMSS-2945]

The Design safety case fits in this realistic scenario by providing an early saf...

The Design safety case fits in this realistic scenario by providing an early safety argument for the later integration without having to wait on the Generic Product and Application Safety Cases. It will ease the later change and evolution processes as the safety requirements are documented independent of the actual products and generic applications used in the integrated system. [SPPRAMSS-2944]

Generic Design Safety Case (GDSC) in the Context of RAMS Phases

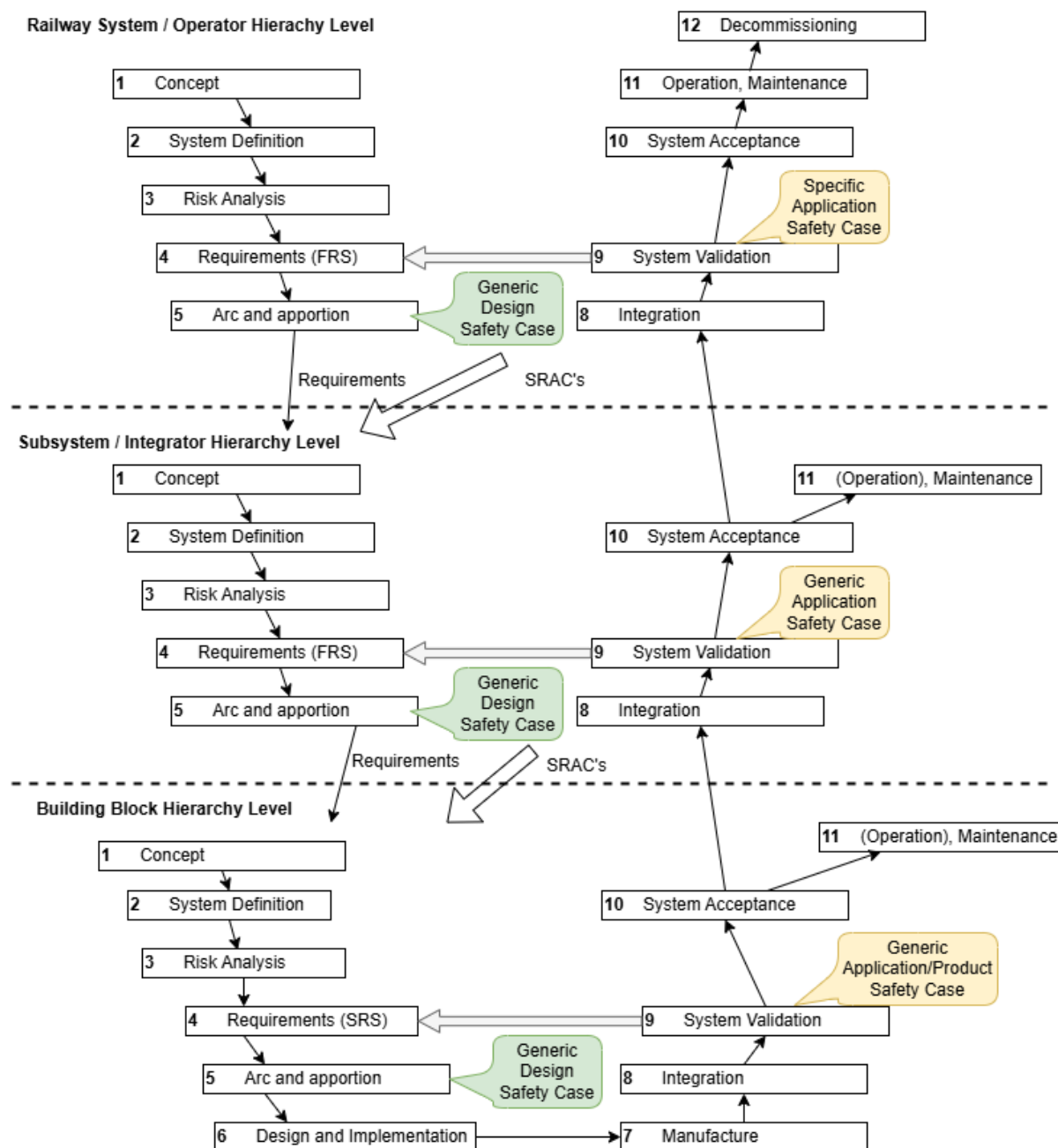


Figure 5 Generic Design Safety Case (GDSC) in the Context of RAMS Phases

5.5 Safety Case Structure for migration and integration of legacy products and applications

Figure # Safety Case Structure with Design Safety Case for migration and legacy s...

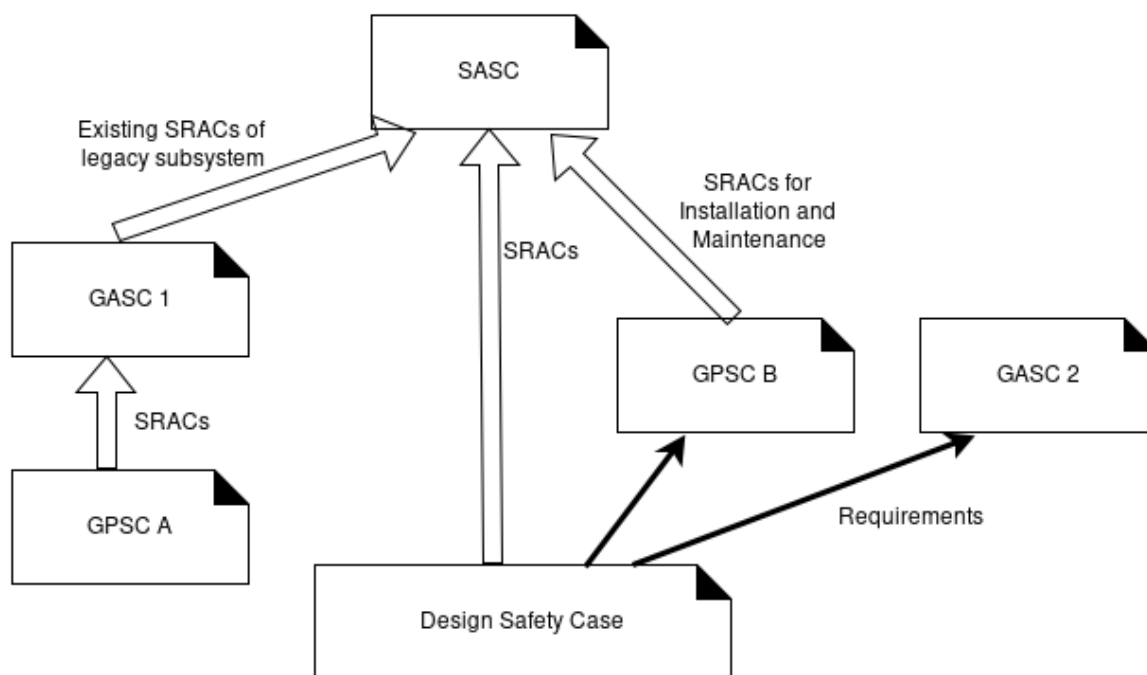


Figure 6 Safety Case Structure with Design Safety Case for migration and legacy subsystems

Integration of existing systems into ERJU safety case structure

It shall be possible to integrate modules developed in the new safety case regime into existing systems by referencing the Design Safety Case for the new products and applications in the SASC while retaining the safety cases for legacy systems. Nevertheless, high integration and certification costs will persist as the Design Safety Case will not be able to show the safety of the resulting system. [SPPRAMSS-416]

5.6 Composition of the Design Safety Case

Structure of Design Safety Case

The Design Safety Case itself shall be composed of safety cases that represent the various functions the system contains. This hierarchical structure allows a work split of the detailed hazard analysis and requirements management activities while providing a central document to provide overall risk analysis, TFFR allocation and SRAC data base. [SPPRAMSS-1321]

Granularity of Design Safety Cases for Functions

The granularity of the Design Safety Cases shall follow the split of functional specifications as well as the foreseen architecture. The goal - as in every System Definition chapter of a safety case - is to find a scope that is well assessable.

Section from EN 50129	Applica ble to DSC	Description or Justification