Rail to Digital automated up to autonomous train operation

D26.4 – Summary of findings and recommendations from study on modular certification and homologation

Due date of deliverable: 31/10/2025

Actual submission date: 04/11/2025

Leader/Responsible of this Deliverable: Oliver Mayer-Buschmann / DB InfraGO AG

Reviewed: Y

Document Status		
Revision	Date	Description
01	03/07/2025	First issue for alignment, contribution and internal review
02	01/09/2025	Internal review revision
03	19/09/2025	Final internal review revision
04	01/10/2025	Submission to TMT
05	04/11/2025	Minor correction after TMT / SteeCo review
06	29/01/2026	Corrections after JU review
07	17/02/2026	Final revision for publication

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU		**X**
SEN	Sensitive – limited under the conditions of the Grant Agreement	

Start date: 01/12/2022 Duration: 42 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe’s Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union’s Horizon Europe research and innovation programme and the Europe’s Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Oliver Mayer-Buschmann	DB InfraGO AG	Chapters 2, 8, Appendix B&C, Editorial, Review
Markus Spindler	DB / Rail Expert Consult	Chapters 4, 5, 6, 7
Julia Gajo	DB InfraGO AG	Chapters 3, Appendix A, Review
Patrick Marsch	DB InfraGO AG	Review
Julian Wissmann	DB InfraGO AG	Chapters 1, Review
Zeeshan Ansar	DB InfraGO AG	Chapter 4
Stefan Resch	Hitachi Rail GTS	Chapter 5
Ignacio Alguacil Ventas	INECO	Review
Patrick Rozijn	NS	Chapter 4,5, Review
Thomas Martin	SBB	Figures, Review
Sonja Steffens	Siemens Mobility	Chapter 4, Review
Thomas Bernburg	Siemens Mobility	Chapter 4, Review
Julien Spanneut	SNCF Voyageurs	Executive Summary, Chapter 4, Review

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

EXECUTIVE SUMMARY

By increasing the automation in the railway sector, including the deployment of fully automated driving, new requirements and expectations arise regarding the different building blocks of modular systems. To address these challenges, this work package – supported by railway companies and industry partners – analysed modular certification approaches for Modular Computing Platforms (MCP).

The purpose of the MCP is to provide an up to SIL4-capable computing platform that enables the decoupling of hardware and software lifecycles and their respective update cycles, while ensuring compliance with railway safety and cyber-security requirements.

This deliverable summarises the findings from the study on modular certification and homologation, including concepts for modular certification and assessment.

The detailed analysis covers:

- The current regulatory landscape and its implications for modular certification.
- The definition of roles and responsibilities for stakeholders involved in certification and homologation.
- The alignment of the MCP concept with Europe's Rail System Pillar from the Computing Environment, Transversal CCS, PRAMS and Cyber-security domains.
- A dedicated analysis of cybersecurity aspects relevant to modular platforms certification.

Based on this analysis, the deliverable presents findings, conclusions and recommendations to support the introduction of MCPs in future railway systems. Key recommendations include the need for an evolution of the regulatory framework and the introduction of clear role definitions.

Finally, this deliverable concludes Task 4 of Work Package 26 and identifies topics for future study, such as the refinement of modular safety cases, deeper integration with Europe's Rail activities, and evolutions of the European railway regulations, in particular the anchoring of MCP needs in future Technical Specifications for Interoperability (TSI) updates.

ABBREVIATIONS AND ACRONYMS

ALPI	Application-level Platform Independence
AsBo	Assessment Body
ATO	Automatic Train Operation
COTS	Commercial Off The Shelf
CCS	Command, Control and Signalling
CSM(-RA)	Common Safety Methods (on risk assessment)
DeBo	Designated Body
ERA	European Union Agency for Railways
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FRMCS	Future Railway Mobile Communication System
HLPI	Hardware-level Platform Independence
HW	Hardware
ISA	Independent Safety Accessor
LRU	Line Replaceable Units
MCP	Modular Computing Platform
MPC	Modular Platforms Concept
NoBo	Notified Body
OCORA	Open CSS On-Board Reference Architecture
OT	Operational Technology
PI API	Platform-Independent Application Programming Interface
R2DATO	Rail to digital automated up to autonomous train operation
RBC	Radio Block Centre
RCA	Reference CCS Architecture
RTE	Run Time Environment
SCP	Safe Computing Platform
SMS	Safety Management System
SRACs	Safety Related Application Conditions
STIP	Standardisation and TSI Input Plan
SW	Software
TSI	Technical Specifications for Interoperability

USE OF TERMINOLOGY

Certification: Both the act of issuing a certificate and the whole process to get there.

Certificate: A document that may result from an assessment or a regulatory decision.

Assessment: Both the process leading to a final judgement and the final judgement itself. Can end in a decision or serve as input for one.

Authorisation: A formal permission, often based on assessments, certificates, and declarations.

Approval: Officially used in some contexts (e.g., “type approval”), especially in railways outside ERTMS.

Homologation: Generic and widely used wording which refers to the entire process comprising all the certificates, assessment reports and authorisations (remark: this is today’s use of the term; historically, it had a more specific meaning not relevant anymore)

Conformity Assessment Bodies: Railway conformity assessment bodies are independent organisations recognised by national authorities to assess whether railway systems and components comply with European Technical Specifications for Interoperability (TSIs) and national technical regulations. Such bodies act as Notified Bodies (NoBo) for the EU or Designated Bodies (DeBo) for national requirements.

MPC: The term Modular Platforms Concept - as introduced in Chapter 3 of the former deliverable D26.3 [5] – is used in this document to refer to the Concept in its entirety, deriving the Specification and Architecture with a consolidated set of high-level platform requirements, introducing three different domains to help with the complexity of the topic: The Application-Level Platform Independence (ALPI) domain – with a strong focus on software and runtime environments, the Hardware-Level Platform Independence (HLPI) domain – focusing on hardware abstraction and virtualisation aspects, and the internal and external interfaces – providing interoperability to the outside and adaptability on the inside of the MPC.

MCP: The term Modular Computing Platform represents in this deliverable all physical equipment and platform software that is described in the architecture of the Modular Platform Specification as introduced in D26.3 [5], focusing on the Compartment Execution Environment (CEME) with Hardware-level Platform Independence (HLPI), and components and interfaces of the Platform Management needed for operation in respect to the certification and authorisation demands, identified and worked out in this deliverable.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This document, inside the framework of the R2DATO project, provides findings and recommendations on the certification and acceptance approaches of modular platforms and the railway functions hosted on them as described in the remits for Task D26.3.

The deliverable describes the approach to modular certification by describing the relevant regulatory landscape in detail, comparing it to the current system breakdown and deriving from there the necessary change introduced with modular platform certification. From there it puts forward gaps and existing issues as well as possible strategies for the certification, assessment and authorization of modular platforms and proposals for change to the regulatory landscape.

The activities that led to the creation of this document are the continuation of this work package's existing deliverables, previous projects such as RCA/OCORA, Shift2Rail and others. Additionally work happening in parallel in the ERJU System Pillar is considered. See chapter 4.5 for details on input documents used.

The partners involved in this project have leveraged their extensive skills and expertise acquired over the years, including their contributions to previous projects and the experience in the certification of proprietary CCS products across Europe. As a result, they have collaborated to create a comprehensive summary, the details of which are discussed in this document.

The goal is to define a procedure for the certification, assessment and authorisation of modular platforms within today's guidelines and frameworks and to point out and develop solution proposals for shortcomings or issues therein that would hinder the introduction of modular platforms.

Within R2DATO, the findings and recommendations on modular certification discussed in deliverable D26.4 are relevant to enable the decoupling of certification concerns in functional safe systems up to SIL4 that are increasingly software-defined and ever more tightly integrated.

The work in this deliverable puts its focus on trackside use cases – as the material provided by the system pillar puts its focus there and most experts of the working group are more familiar with it – however this does not limit its conceptual applicability also to the on-board domain.

1.1 Document Structure

The following table outlines the document structure of this deliverable.

Table 1: Document Structure

§	Title	Description
1	Introduction	Provide an overview of the entire document. Objective, problem to be solved, input from previous projects and work packages, result and value added, other deliverables to which results will be input. Guidance about the document and its structure.

§	Title	Description
2	Scope and Motivation	Provide motivation for this work, its objectives and problems to be solved. Inputs from previous projects and work packages.
3	Approach	Describe the activities performed for obtaining this document.
4	Current Legislatory Landscape in Context to the MPC	This chapter provides an overview over the European Regulatory Landscape, its directives and safety related methods, specifications and requirements for certification and authorisation of organisations, onboard and wayside assets and products, interoperability constituents, etc., as of prior to EU-Rail and puts them in context with the MPC. It connects this with investigations and analysis from the different working groups on integration roles, activities and relevant documents to be created on constituents introduced in former deliverables of WP26 and work done on the certification topic in other contexts.
5	Modular Certification Approaches for the MPC	This chapter motivates the introduction of modular platforms into the railway system and analyses, in detail, the impact of modular platforms on certification and authorisation: name the desirable changes to constraints and limitations to allow for modular certification and authorisation, interchangeability of railway applications and platforms; identify preconditions to develop high-level modular certification approaches.
6	Analysis	Impact analysis of modular platforms on certification and authorisation: desirable new methods and elements. Analysis

§	Title	Description
		on which new forms of modular certification and authorisation would be required to allow interchangeability of railway applications and platforms and develop high-level modular certification approaches
7	Recommendations	This chapter summarises results from the analysis to provide recommendations on how MCPs can be introduced.
8	Conclusion	In this chapter conclusions are summarized, achievements and lessons learned are documented.
	References	Provides relevant references used throughout the document.
A	Appendix	Provides a general overview of the European regulatory landscape, the relevant directives, regulations, standards and guidelines, their hierarchy and binding force.
B	Appendix	Presents the actors that have been identified during the analysis, their responsibilities, relevant activities and main obligations in respect to certification and authorisation to Railway functions and subsystems hosted on the MCP
C	Appendix	Analysis of different integration and maintenance roles and activities in the context of the MPC based on the Modular Platforms Architecture and the scenarios provided by the System Pillar CE “document Operational Analysis Specification”.

1.2 Limitations

On-board specific considerations require further study since they could not be considered in detail during the analysis of this deliverable. This might induce additional aspects or may result in other specific conflicts with existing regulations.

1.3 Existing and Relevant Documents

As input to the Work Package 26 process, the state of the art was considered and deliverables from past projects were identified and actively requested at the Work Package level. For this process, inputs were collected and integrated from relevant Deliverables of R2DATO as well as from several System Pillar Domains.

Doc-1 ERJU System Pillar – Common Business Objectives [2]

Doc-2 ERJU System Pillar, Computing Environment – Deliverable "Recommendation on interfaces to be standardised [9]

Doc-3 ERJU System Pillar, Computing Environment – Deliverable "Operational Analysis Specification" [10]

Doc-4 ERJU System Pillar, Computing Environment – Deliverable "System Analysis" [11]

Doc-5 ERJU System Pillar, PRAMS – Deliverable "PRAMS Plan - Evolution management of safety-related modular systems - Process and organisation" [13]

Doc-6 ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.1 "High level Consolidation" [3]

Doc-7 ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.2 "Intermediate specification of the Modular Platform" [4]

Doc-8 ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.3 "Final Modular Platform requirements, architecture and specification" [5]

Doc-9 ERJU System Pillar Cyber Security - Secure Communication Specification v1.0 [12]

Doc-10 ERJU System Pillar Cyber Security - Secure Component Specification v1.0 [12]

Doc-11 ERJU System Pillar Cyber Security - Security Program Requirements v1.0 [12]

Doc-12 ERJU System Pillar Cyber Security - Shared Cybersecurity Services Specification v1.0 [12]

Doc-13 NIS 2 (Directive (EU) 2022/2555) [18]

Doc-14 Cyber Resilience Act (Regulation (EU) 2024/2847) [19]

Doc-15 Multiple EU Directives and Regulations used for the analysis, listed in Appendix A Table 5

2 SCOPE AND MOTIVATION

The Europe’s Rail Mission and Objectives [1] as defined in ERJU System Pillar Task 1 Railway System are demanding “to deliver a high capacity integrated European railway network by eliminating barriers to interoperability and providing solutions for full integration, covering traffic management, vehicles, infrastructure and services, aiming to achieve faster uptake and deployment of projects and innovations.”

A more detailed breakdown, represented by the ERJU Common Business Objectives [1] is elaborating on concrete goals, addressing modularity and the need for optimisation of safety and security strategies and standards to achieve concrete steps towards a digitalised, connected, more automated, interoperable, and modular technical railway system, as (non-exhaustive extract):

- seamless operations, allowing rail to better serve customer needs
- improved efficiency of the rail system and reduced overall lifecycle costs
- harmonisation to be implemented across the whole EU rail system, improving performance and capacity
- enabling higher sustainability and resilience in public transport
- supply and improve EU rail industry competitiveness supporting the transformation of the current rail system into a central transport mode of tomorrow’s European mobility
- a harmonised approach to evolution and greater adaptability improving the rate of deployment of new technologies

It is clearly stated there that “the sector needs less complexity, higher grade of automation, information integrity, simplicity and flexibility for continuous modular optimisation”. The claim to improve availability, reliability, robustness, sustainability and resilience while simultaneously saving costs and accelerating the rate of new deployments can for sure be considered as challenging.

This is especially problematic, where the need for harmonised evolution and greater adaptability for innovation is conflicting with an existing complex and long lifetime railway system. Integrating old technology and monolithic subsystems, that have been developed based on a regulatory landscape that has not been evolved to target the demands and objectives raised above, will make it necessary to implement changes in the future.

Many aspects of the Common Business Objectives have been considered driving the standardisation activities in the System Pillar. Work results such as a proposed Computing Platform Architecture, Interface Definitions and alignment towards harmonised operations, have been developed in the SP Computing Environment domain and got integrated into the Modular Platform Specification work of R2DATO WP26. Multiple above-mentioned demands are directly or indirectly well supported by the Modular Platform Concept, as introduced in the deliverable D26.3 [5] (e.g., chapters 3.1 Purpose and 3.4. Goals & Non-Goals).

High rates of new deployments combined with RAMS and security requirements for a 24/7 operation need appropriate support by optimised certification, authorisation processes that are introducing new roles and accountabilities. This deliverable aims to analyse and conclude on concepts for the needed certification, integration and maintenance of relevant constituents of the Modular Platform, by analysing preconditions, inputs, roles, accountabilities of relevant stakeholders and the existing regulatory landscape. Setting focus towards the ability to integrate and operate the needed railway applications in a range from SIL4 down to Basic Integrity, the implementation of safety-related functional systems, software-based railway equipment requires a deep analysis of specific Modular Platform use cases with the aim to develop concrete recommendations, considering guiding principles from the SP PRAMS domain. The main goal is to pave the way towards a modular, scalable, sustainable and cost-effective roll out and operation of CCS systems and CCS related applications for both, deployments in data centres and rolling stock.

2.1 Deliverable Objectives

In the continuation of the former WP26 Deliverables where the project partners have worked out specifications along the MCP architecture, this deliverable pursues the following goals in accordance to the Grant Agreement:

- High level top-down view on Modular Platforms in the context of the existing Regulatory Landscape and that needed in the future
- Inside view on the Modular Platform, its relevant constituents and derived activities needed in the context of certification and authorisation, integration and maintenance

The main deliverable objectives can be summarised as the following:

D26.4-O1 Capture the current Regulatory Landscape on certification and authorisation of Railway systems to outline the existing legal framework and identify the most important European regulations determining and impacting the future authorisation of Functional Systems deployed on Modular Platforms

D26.4-O2 Identify and analyse relevant preconditions, processes, needed inputs, integration and maintenance scenarios and impacted interfaces. Propose involved stakeholders and derive related roles and activities and resulting outputs, constituting a trust model for all involved stakeholders

D26.4-O3 Provide findings and work out concrete outcomes and recommendations, potentially adapting parts of the regulatory landscape to support the Modular Platform Concept (MCP) and paving the way for future realisations and rollouts in data centres and rolling stock on-board deployments

D26.4-O4 Feed insights and results back into the standardisation activities of the System Pillar Computing Environment and PRAMS domains to enable evolvability and cost control for the utilisation of Modular Platforms, with the objective to improving the deployment rate of new technologies in the Railways

D26.4-O5 Define the scope and preconditions for Modular Platforms to outline and enable authorisation approaches that may be further developed in future R&I projects and standardisation. This objective supports higher TRL activities by providing guidance and a structured trust model intended for application in real test environments beyond the scope of this deliverable.

3 APPROACH

This chapter describes the overall approach towards this deliverable, the workflow that has been created, and how the content and results have been achieved.

To understand certification for a modular, multi-vendor computing platform, we first need to review the current European legislation and standards. This has therefore been the starting point of our work. We began by creating a clear picture of which regulations, norms, and standards are relevant, followed by defining which of those should be discussed further in the ongoing work to establish a clear scope. This led to a description of the regulatory landscape, including the major standards, norms, and regulations (see chapter 4.3). This work has formed a basis which, in the later stages, has been used to identify both gaps and opportunities in the current legislation. It has furthermore provided insights into the various roles and responsibilities described within the current framework.

The work then progressed towards the structure of the actual computing platform. It became clear that the responsibilities defined in the current legislation are divided in a certain way, which must somehow be mapped to the architecture of a modular, multi-vendor computing platform. The second step in our work was therefore to assess the architecture of the computing platform in relation to certification. A group was initiated to map the platform architecture to roles and responsibilities of different actors, based on Deliverable 26.3 [5], focusing on roles and responsibilities that will be necessary for future certification. This work also included discussions about the obligations of different actors during the various stages of the two most relevant life cycle phases, integration and maintenance. At this stage, it became evident that the architecture strongly influences how certification steps and boundaries should be defined. This subsequently led to discussions and the development of a workflow in which the different actors had to be linked to the various integration steps. The focus then shifted towards defining the necessary tasks of the involved actors to move closer to understanding how responsibilities are divided; an essential aspect of determining how certification processes could be structured.

Following this, it was possible to identify whether there are constraints in the current regulatory framework that hinder the certification of a modular, multi-vendor computing platform. In a final step, initial indications were made regarding which necessary changes should be further investigated. This includes suggestions for what might need to be implemented in future legislation.

4 CURRENT LEGISLATORY LANDSCAPE IN CONTEXT TO THE MPC

4.1 Introduction

This chapter serves to give a short introduction on the current situation for the relevant topics discussed in this deliverable, to give the reader the relevant background information and context. The legislative and regulatory landscape described in this chapter is primarily governed by the European Union railway interoperability and safety framework. In particular, Regulation (EU) 2016/797 on the interoperability of the rail system within the European Union and Regulation (EU) 2016/798 on railway safety provide the overarching legal basis. These regulations are complemented by relevant Technical Specifications for Interoperability (TSIs), national rules, and guidance documents issued by the European Union Agency for Railways (ERA), which together form the framework within which Functional Systems deployed on Modular Computing Platforms (MCPs) must be certified and authorised. The chapter will first explain shortly the relevance of the Modular Platform Concept (MPC), as it is the basis of the ongoing work within the work package, then lead over to give a short introduction to the current Legislatory Landscape. Following that, we will provide the link between the Modular Platform and the current Legislatory Landscape and why there is a need to dive into that topic. Moreover, this chapter is providing an overview of the current work related to the topic within the SP. This is done to make the reader aware of the different activities going on in this context and how these activities are related to this deliverable.

At the end of this chapter the reader is expected to have gained an overview of the current specification for the Modular Platform and where topics are touched in the context of the current legislation.

We strongly advise the reader to get background knowledge on the MPC before diving into the topic of certification as the architecture of the Modular Platform is crucial for the work which is discussed in this deliverable. To do that, please study the Deliverable D26.3 [5] “Final Modular Platform requirements, architecture and specification”.

4.2 MPC Relevance

The MPC offers, among else, new economic opportunities for deployment and maintenance of software-based railway equipment. To better understand this, it is helpful to differentiate software-based railway equipment into two categories:

Case-A) Software-based railway equipment which has a direct functional interaction with physical interfaces (like motors for point machines, barrier levers at level crossings, light points in signals, axle counter sensors, antennas for balise detection, train driver HMIs). Such equipment necessarily has a physical part to its intended functionality and thus the MPC in general is less relevant in this case.

Case-B) Software-based railway equipment which has only data-based in- and output (no physical functions), while still implementing logical functions and a business logic. The in- and output is conveyed to other components of the railway system by IT network infrastructure. Here, the physical level can be abstracted (to bandwidth requirements, transmission times, response times, concurrency requirements etc.). Such equipment can separate (to a reasonable degree) the logic of the functional system from the physical infrastructure of the computing platform executing the logic. With that separation it is possible to explicate the requirements the logic depends on to be safely executable. Today, such systems often still are provided as systems consisting of (specific) hardware and software with system certification (i.e. certification comprising the explicitly defined and integrated HW/SW system), hardware is thus currently mostly vendor-specific. In future, such systems could and should (from an economic as well as from a product life cycle point of view) be provided as system software, running on a (COTS) computing platform.

Today, Case B) is technically covered in differing depth by the major suppliers of railway equipment, even to the point of deploying the functional system in virtualisation environments.

The MPC is covering Case B) by a harmonised approach. This is mainly realised by a standardised interface between the software-based Functional Systems and the CEME as introduced by the System Pillar Computing Environment deliverable "Recommendation on interfaces to be standardised" [9] and D26.3 [5].

From the perspective of the MPC, the question is whether the full potential of the MPC, in terms of economic opportunities, technical capabilities and lean processes for authorisation of deployment, maintenance and evolution can be realised under the currently given regulatory framework. This question is investigated in detail in chapter 5. For basic orientation in this topic,

- the following Section 4.3 introduces the current regulatory framework affecting authorisation of deployment, maintenance and evolution of railway equipment.
- Section 4.4 defines the main actors named in the current regulatory framework and are involved (to some degree) in the authorisation of deployment, maintenance and evolution of railway equipment.

4.3 Regulatory Landscape

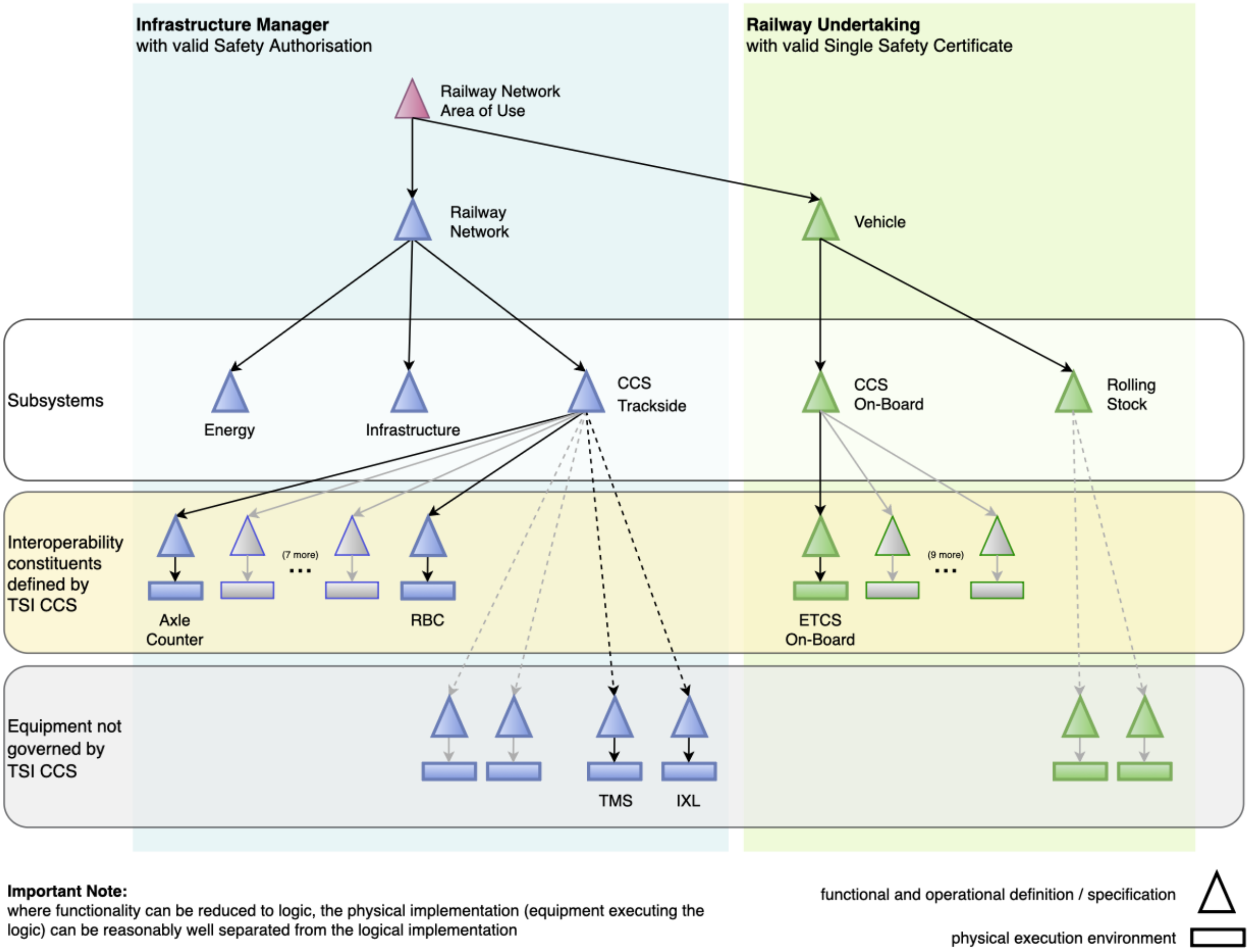
Certification is at the heart of interoperability. The path of harmonisation of European railway is closely related to certification, which is easily illustrated when we trace how the interaction between rolling stock and infrastructure has evolved from fragmented, national approaches towards harmonised European processes. This is described in more detail in Appendix A.

At the end of this evolution, a number of European Directives and Regulations have emerged, which govern safety and interoperability of the European railway network. Appendix A describes these Directives and Regulations and discusses their relations among each other, to give an insight on how authorisation and certification of railway equipment is organised from a top-down perspective.

In a nutshell, today the European railway network is subject to several European Directives and European Regulations covering safety and interoperability. These topics are broken down to the technical level by technical specifications for interoperability (TSI) in order to harmonise the sector. Railway equipment which is not directly related to interoperability of the vehicles and the network are only affected by the safety aspect. This matter is less strictly broken down to the technical level, as the overall safety is explicitly under the responsibility of the main actors, the railway undertakings and infrastructure managers.

4.3.1 Railway System Structure from the Perspective of Authorisation and Certification

Figure 1 provides an overview of how the Railway System is currently structured from the perspective of these directives and regulations:


Infrastructure Manager
with valid Safety Authorisation
Railway Undertaking
with valid Single Safety Certificate
Railway Network Area of Use
Railway Network
Vehicle
Subsystems
Energy
Infrastructure
CCS Trackside
CCS On-Board
Rolling Stock
Interoperability constituents defined by TSI CCS
(7 more)
(9 more)
Axle Counter
RBC
ETCS On-Board
Equipment not governed by TSI CCS
TMS
IXL
functional and operational definition / specification
physical execution environment

Important Note:
where functionality can be reduced to logic, the physical implementation (equipment executing the logic) can be reasonably well separated from the logical implementation

Figure 1: Railway System structured from the Perspective of Directives and Regulations

4.3.2 Relation of the MPC to the Structure of the Railway System

4.3.2.1 Problem Statement

Modular Computing Platforms are related to the structure described in the Figure 1 implementing the physical execution environment. If they are used on a system-by-system basis like in Figure 1 this is fully compliant to current legislation.

However, if execution of several Functional Systems on top of one MCP would be attempted under the current regulatory framework, the result would be a situation where the MCP would be subject to several certificates and safety cases in parallel at the same time, making it almost impossible to establish contracts between and safety management across the different involved organisations to meet the legal requirements.

This is because at that layer, today, railway equipment is seen as fully integrated hardware + software systems, which are certified together (i.e. certification comprising the explicitly defined and integrated HW/SW system).

As described before, software-based railway equipment, which only exchanges data through interfaces, does not need to be locked to any specific hardware (seen both from an economic as well as from a product life cycle point of view). Such equipment should instead be provided as a system software running on a (COTS) computing platform. The MPC describes such a platform, in a harmonised way.

4.3.2.2 How the computing platform of software-based railway equipment is addressed in certification and authorisation today

When the MPC is used for physical implementation of railway equipment in today's regulatory landscape, the MPC can be:

- part of the system under consideration for certification or
- part of the system under consideration for the safety case

(or both).

Right now, when railway software is certified, the exact hardware it runs on (hardware, OS, firmware, version, and configuration) is stated in the certification documents. Regulations then strictly control what happens if anything changes. Even small updates may require new documentation or re-certification. Because of this, the choice of computing platform, and its specific version, directly limits where and how it can be used.

From the perspective of the MPC, the question therefore is whether the full potential of the MPC, in terms of economic opportunities, technical capabilities and lean processes for authorisation of deployment and maintenance can be realised under the currently given regulatory framework.

4.3.2.3 Ease of use of COTS products under the current regulatory framework

The use of commercial off-the-shelf (COTS) products is encouraged in principle, but in practice each case is treated separately, every certification and every safety case is handled on its own. This leads to inefficiency and a lack of harmonisation, both in technical terms and in the related processes of assessment, certification, approval, and authorisation.

To fully realise the potential of the MPC, one key element is still missing: a harmonised framework for how to efficiently and consistently deal with COTS hardware, COTS software, and their suppliers.

4.3.2.4 Current system breakdown for the purpose of certification

Finally, we briefly discuss the structure illustrated in Figure 1, to understand the current regulatory framework (as mentioned, the MPC directly relates only to the lowest layer).

The current legislation divides the railway system into 3 different levels, which are utilised for certification. The *system level***,** which can be seen as the top-level classification category, is about ensuring that the organizations running the railway system are competent and operate safely, while *the interoperability level* is about making sure that all the technical parts can work together seamlessly across the European network. The last level of this classification is the *subsystem level* (primarily derived from the TSI CCS Regulation (EU) 2023/1695) including the actual assessment and thus certificates that are issued on the specific product. All approval processes, risk management activities, and technical checks required by regulation can be mapped to one of these three levels. This distinction is of importance for understanding how responsibilities, processes, and compliance requirements are structured within the sector. At the same time the framework itself is used differently across European countries, enabling some to carry out less complex certification procedures, while others operate with very complex approaches.

The most relevant level for the MPC (and this document) is the subsystem level, where the detailed system breakdown is defined by TSI CCS and where the manufacturers get involved into processes and responsibilities towards the railways. This involvement is sketched to some detail in the respective table in Appendix B.

The three levels mentioned above may appear very abstract and are thus shortly explained with concrete examples:

System Level

Explanation

The System Level covers all requirements, certifications, and processes that apply to the overall management and safe operation of railway infrastructure as well as rolling stock by RU’s. This level is primarily concerned with the organizational and procedural aspects necessary to ensure the safe functioning of the railway system as a whole.

On this level, the regulatory framework also covers how significant changes to the railway system are managed. These processes are essential prerequisites for maintaining system integrity over time and are of particular relevance in the context of MPC certification. When an organisation plans a substantial technical or operational change, it must follow established configuration management procedures and conduct a risk assessment in line with the Common Safety Method for Risk Assessment (CSM RA). In some cases, the ERA can be asked for a technical opinion on safety or interoperability aspects, supporting national authorities in their decision-making.

Example

For example, infrastructure managers are required to obtain a safety authorisation from the relevant National Safety Authority. This authorisation is only granted if the infrastructure manager can demonstrate that it has established and maintains a safety management system (SMS) in line with European safety standards, complying with the requirements set out in Article 9 of Directive (EU) 2016/798 [13] in compliance with the requirements set out in Annex A or Annex B of the CSM on SMS [17]. Similarly, railway undertakings must hold a single safety certificate, typically issued by the European Union Agency for Railways (ERA), confirming that their safety management systems are compliant and effective.

Interoperability level

Explanation

The Interoperability level is covering the main processes and certificates to be achieved for technical systems to work seamlessly together, in a sense of „vertical separation“ on the functional architecture level. This level is at an abstraction level which is still very high and not going into detail for specific subsystems or components but basically includes the overall terms of rolling stock as well as infrastructure and then refers to the systems being compatible with TSI's as well as having used the CSM. This is said while not including the normative thread described and outlined by CENELEC for example. With respect to the MPC, this level is of very indirect relevance, as the MPC is agnostic of the functions performed by the functional systems executed on the MCP. But, as long as the involved technical systems are described down to the level of the used computing platform in the documentation for authorisation, actions will always affect the authorisation of the technical system, often blocking these actions without any benefit for interoperability or safety.

Example

For instance, before a rolling stock can be used, it must be authorised, registered, and assigned to an entity responsible for its maintenance. The process also includes checks to ensure that the vehicle is compatible with the intended route and that it can be safely integrated into train operations. Trackside installations, such as signalling systems (including Command, Control, and Signalling (CCS) subsystems), require formal authorisation before they can be commissioned. This involves verifying that all technical, safety, and interoperability requirements are met, often through a combination of declarations of verification, technical documentation, and conformity assessments.

Subsystem level

Explanation

In Directive (EU) 2016/797, Article 2 (5) and Annex B, 'subsystem' means the result of the division of the rail system into structural or functional parts; these subsystems are structural (infrastructure, energy, trackside control-command and signalling, on-board control-command and signalling, rolling stock) or functional (maintenance, telematics applications for passenger and freight services). At this level, the directive specifies the processes for authorising the subsystems of interest before they can be placed on the market or put into service.

Annex B, Article 2 states: "For each subsystem or part of a subsystem, the list of constituents and aspects relating to interoperability is proposed by the Agency at the time of drawing up the relevant draft TSI.". Within article 4 'Content of TSIs' it is also stated that each of the subsystems defined in Annex B shall be covered by one TSI. Where necessary, a subsystem may be covered by several TSIs and one TSI may cover several subsystems. The MPC is for example subject to the TSI CCS and the structural/functional breakdown of the CCS (control-command and signalling) subsystem related to it, and to the TSI LOC&PAS if deployed on-board.

Example

Certificate of Verification, approved by a Notified Body (NoBo) who checks and certifies that the subsystem complies with the relevant technical specifications for interoperability (TSI), also cover verification of the interfaces of the subsystem in question with the system into which it is incorporated. The subsystems in place can be electronic and physical systems that manage train movements, such as ERTMS on-board and trackside equipment (example on: ERTMS On-Board Subsystem Certification).

4.4 Definition of Roles and Responsibilities

The current regulatory framework defines actors to be considered in authorising and operating railway systems and parts thereof. These actors have different activities and objectives on system level, interoperability level and subsystem level. Here, we give an overview of which of the actors mentioned in the cited EU directives and regulations are relevant for the purpose of this deliverable; in Appendix B we go into more detail and show their respective objectives in the different system breakdown levels.

Table 2: Relevant Actors

Actors relevant in the context of this work	
Top actors defined in Directive 2016/798 on railway safety	ERA NSAs Railway Undertakings Infrastructure Managers Entities in Charge of Maintenance
Additional actors defined in Directive 2016/797 on the interoperability of the rail system	(Vehicle) Keepers Notified Bodies (NoBo's) Manufacturers
Additional actors defined in Regulation 2018/545 on railway vehicle authorisation and railway vehicle type authorisation process	Holder of the vehicle type authorisation
Roles defined in context of the conformity assessment and authorisation processes (Regulation (EU) 2019/779)	Proposer Applicant Authorised Representative (of a manufacturer) Contracting Entities

Table 3: Actors currently of no further Relevance

Other actors (not relevant in the analysis of this document)	
Bodies not relevant in the analysis of this document. All named roles are defined	Accident and Incident Investigating Bodies Directive (EU) 2016/798 Designated Bodies (DeBo's) Directive (EU) 2016/797

Other actors (not relevant in the analysis of this document)	
in the respective regulatory texts.	National Accreditation Bodies ISO/IEC 17011 National Recognition Bodies NB-Rail coordination group Regulation (EU) 2016/796 (ERTMS group of notified conformity assessment bodies)
General actors not further specified but named in Regulation (EU) 2019/779	Service Providers Maintenance Suppliers
Actors in relation to transport of goods, defined in Directive (EU) 2016/798	Consignor, Consignee Loader, Unloader Filler, Unfiller Carrier

These actors have different obligations on the different levels of system breakdown. Refer to Appendix B for an overview for each of the different system levels.

Key take away to keep in mind:

"The main actors in the Union rail system, infrastructure managers and railway undertakings should bear full responsibility for the safety of the system, each for their own part. Whenever appropriate, they should cooperate in implementing risk control measures." [Directive (EU) 2016/798, clause (7) of the introduction]

From the perspective of the MPC, the question is whether the full potential of the MPC, in terms of economic opportunities, technical capabilities and lean processes for authorisation of deployment and maintenance can be realised with this set of actors and their obligations defined as is, or whether including other or additional actors promises benefits. The subsequent sections of the document investigate this question.

4.5 Alignment with ERJU System Pillar Activities

The Europe's Rail Joint Undertaking (ERJU) System Pillar (SP) Computing Environment (CE) domain is working on modular computing environments for railway. The domain's goal is a holistic top-down approach, staying agnostic to implementation details and especially towards trackside and on-board differences[1]. So far, the domain has released two deliverables: "Recommendation on interfaces to be standardised" [9] (referred to as "RIS" in this chapter) and "Operational Analysis Specification" [10]. Furthermore, the domain is maintaining the glossary. Both documents and the aligned glossary are crucial inputs for the Modular Platform Concept in work package 26 and build its basis.

[1] For example, so far, the SP CE domain did not touch on-board specifics, such as IO needs and interfacing to specialized hardware that would still be considered COTS, albeit not in the form of "standard servers", as there are standard on-board hardware systems available from some suppliers.

Other domains of relevance are the SP PRAMS domain, the SP Cyber-Security domain and the SP Transversal CCS (TCCS) domain. The alignment has been captured in dedicated subchapters of D26.3 [8].

4.5.1 ERJU SP CE Domain

The SP CE domain recently performs the system analysis of Computing Environment (CE), which contains a logical layer architecture that highlights the system under consideration, external systems, actors, capabilities, and functions. The focus of the architecture is to clearly define the subsystem and its interfaces to enable modularity and ease of homologation. Furthermore, in the system analysis document the system operational context and CE operational scenarios are discussed, which include execution, deployment, update and recovery

System scenarios detail the system functional structure by defining and grouping system functions and requirements into subsystems. The system architecture has been described in a way that utilises the standardised interfaces and processes that allow for specifying the system's homologation structure. The supplier of the component must provide evidence of compatibility through approval documents and corresponding certification.

The working groups of this task have used those operational scenarios for their analysis related to certification and authorisation in the context of the MPC, deriving relevant input, output documents, roles, accountabilities, responsibilities and activities of involved actors. Examples are provided in Appendix C.

The SP CE domain is currently working on the specifications of I2-Hardware abstraction and I3-virtualisation interfaces, which will provide the detailed computing platform specifications through defined APIs and requirements. The specification will cover standard COTS components such as virtualisation and compartment management, and special components such as native hardware access. The specification will analyse the possible implementation of NHA and standardisation of NHA data models.

Based on the input of the SP CE domain, this document analyses the operational scenarios and details the needed requirements and steps to pave the way for the modular railway system homologation, including subsystems, interfaces, actors, and responsibilities for all operational scenarios, integration, deployment, update, and recovery defined by SP CE.

4.5.2 ERJU SP TCCS Domain

The System Pillar Transversal domain is currently working on the interface specifications of configuration and diagnostics (SMI, SDI) of the CCS system. The Configuration Management and Diagnostics specifications defined by the SP Transversal domain introduce the building block configuration concept for standardised maintenance of a modular system. The Service Functions Configuration and Diagnosis relate to the PRAMS evolution management for safety-related modular systems, outlining a structured approach for handling updates that provides a standardised method for managing system evolutions.

SP TCCS domain conducted a risk analysis based on the FMEA (Failure Modes and Effects Analysis) to ensure the safety of the end-to-end data process life cycle. Based on the FMEA, the safety requirements are formulated for the service configuration function.

As the SMI and SDI Interface specifications are used for the deployment, configuration, and update of the CE, their implications for railway system operations and approval need to be addressed.

4.5.3 ERJU SP PRAMS domain

The alignment with the PRAMS domain has been established during Task 26.3, by personal relation (two members of the ERJU SP PRAMSS domain joining the WP 26 team) as well as by exchange on the key documents already published.

The SP PRAMS domain is in charge of defining the strategy, policies, methods, and principles to be followed by the other Tasks and Domains during the design activities as well as coaching and supporting implementation, in particular:

- PRAMS Assurance Processes definition
- PRAMS standardisation and PRAMS breakdown to components
- Application standardisation, PRAMS framework

Process definitions detail the templates for Hazard and Risk Analysis and coordination with the Engineering Environment Team to align with System Engineering Management Plan (SEMP); Harmonized hazard lists for Operation and System level; a proposal of possible changes to CENELEC standards starting with EN 50126, 50716, 50129 to better support harmonisation and modular approaches.

A PRAMS breakdown to components details the system functional structure by perspective of PRAMS management, assessment and approval needs.

The SP PRAMS domain is currently, among else, working on deliverables:

- “Evolution management of safety-related modular systems - Process and organisation [13]”
- “Safety Case - Strategy for Generic Design Safety Cases” [14].

The deliverable at hand analyses the currently valid homologation process, including subsystems, interfaces, actors, and responsibilities together with the resulting system break down, with respect to its applicability for leveraging the operational and economic advantages of a Modular Platform Concept; this is of direct relevance to the assurance process and PRAMS system breakdown defined by SP PRAMS.

It is important to highlight that there are two different aspects driving authorisation and approval activities:

- Risk management (covered by the PRAMS related activities, assessments and authorisations) and
- Interoperability management, ensuring interoperability and by this enabling a single European rail area (covered by the conformity related activities)

Both have their dedicated assessment bodies and approval and authorisation processes; the current deliverable has its focus on the conformity activities while the PRAMS domain has its focus on the PRAMS related activities, while both need to complement each other without doubling work on specific topics.

4.5.4 Cybersecurity

The Security Domain within Europe’s Rail System Pillar provides the framework to ensure that cyber and information security aspects are consistently addressed across all system development and integration activities. Security requirements are coordinated at a central level, covering the top-level design principles as well as the assurance of their implementation in the System Pillar tasks. This central coordination also extends to the specification of subsystems for security monitoring and for system access control management.

This includes:

- Defining security strategies, policies, and methods in cooperation with the various Tasks and Domains.
- Establishing top-level security definitions, from the current baseline to the target future state.
- Defining a certification process for security at both system and component level.
- Assuring that security requirements are implemented within the System Pillar tasks.
- Contributing to the integration of security requirements into the overall system requirements in line with the SEMP.
- Coordinating and supporting Tasks and Domain Teams in embedding security requirements.
- Specifying tools and solutions for system monitoring from a security perspective.
- Specifying tools and solutions for access control management.

The Security Domain ensures that security considerations are embedded by design, harmonised across the programme, and verified consistently, supporting the delivery of a resilient and trusted European rail system.

The ERJU SP Cybersecurity group has published several documents and guidelines for usage within the Rail domain/industry. It currently hasn't been decided yet how these documents are going to be introduced and used in the next TSI CCS (2028-2030 which is going to introduce cybersecurity requirements and the new specification of FRMCS (v3). This will certainly have an impact on certification and homologation of the Computing Environment.

In addition to the documents published by the SP Cybersecurity group the European Union has also published legislation for cybersecurity which is also applicable to the Rail domain.

5 MODULAR CERTIFICATION APPROACHES FOR THE MPC

For software-based railway equipment which has only logical in- and output (i.e. no physical functions), where the in- and output is conveyed to other components of the railway system by IT network infrastructure, the physical level can be abstracted (to bandwidth requirements, transmission times, response times, concurrency requirements etc.). Such equipment can separate the logic of the functional system from the physical infrastructure of the computing platform executing the logic. Other industries by now have taken advantage of this opportunity and execute such software in highly performant virtualisation environments, offering higher resource efficiency, higher ease and better economics in maintenance plus better RAM performance. The financial sector is deploying such systems in large scale even for software-based systems bearing very high financial risks if failing severely.

The MPC is a railway sector approach to provide such a computing platform with harmonised interfaces, services and processes for deployment, operation and evolution. We present the following Figure from D26.3 here again as an illustration for the all over architecture, in particular introducing the separation between Functional Systems and the underlying Compartment Execution Environment (and Platform Management).

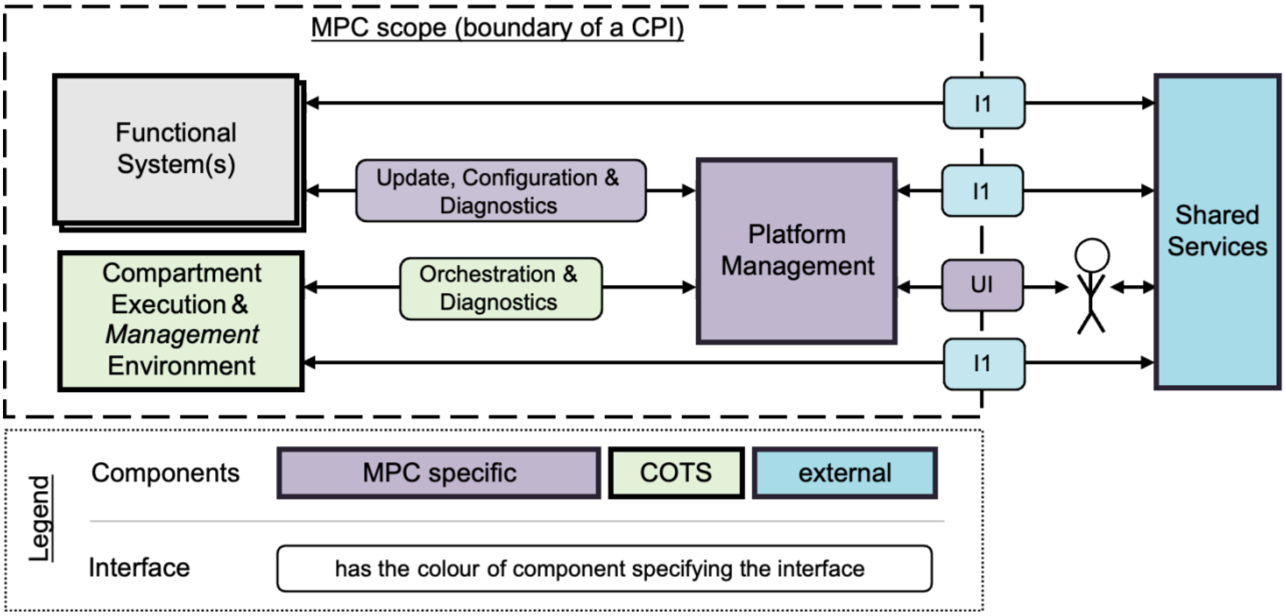

MPC scope (boundary of a CPI)
Functional System(s)
Update, Configuration & Diagnostics
Platform Management
Compartment Execution & Management Environment
Orchestration & Diagnostics
I1
I1
UI
I1
Shared Services
Legend
Components
MPC specific
COTS
external
Interface
has the colour of component specifying the interface

Figure 2: High Level MPC Service Architecture

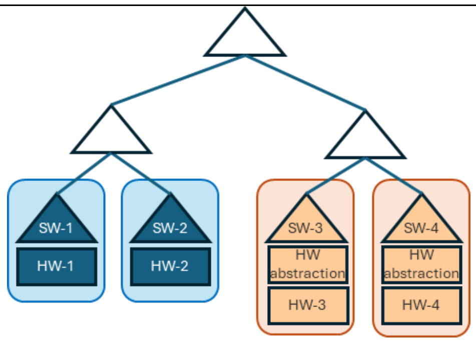
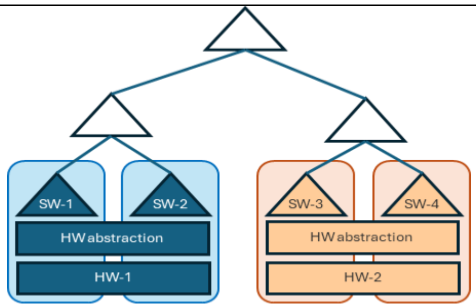
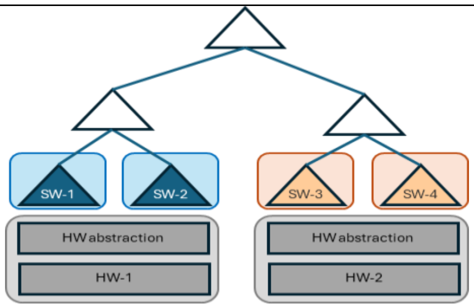
As we have seen in the sections before, if interoperability or safety relevant functions are executed in the software-based system executed on a computing platform, the software-based system is subject to certification and/or safety assessment. As long as the computing environment executing the software is considered as an integral part of the software-based system, the computing platform is subject to certification and safety assessment as well.

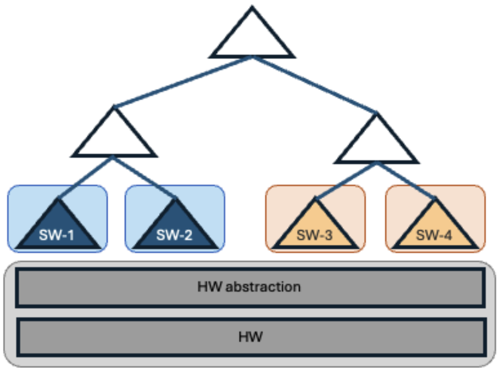
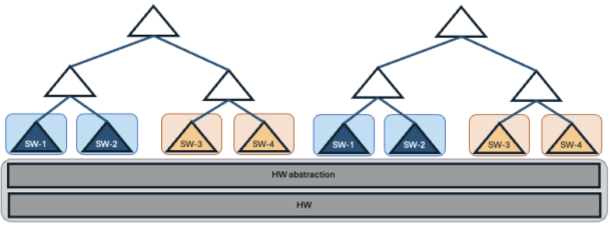
Separation of the software and the computing environment in the considerations for interoperability and safety is possible to a certain extent and is realised today partly by some suppliers, on a product-by-product basis.

The computing environments are operated most often by the IM or RU using them, sometimes by the suppliers of the software-based systems. Sharing of resources across software-based systems or even across software-based systems of different suppliers faces high hurdles as responsibilities tied to different certificates and/or safety cases then are effective in parallel on the same system under consideration. This mandates a very high degree of coordination in maintenance and evolution of that systems under consideration and demands a strong agreement on how system failures are handled between the affected systems and stakeholders.

The following figure gives an overview over possible options for deployment structures and responsibilities on interoperability constituent level:

Table 4: Possible Options for Deployment Structures and Responsibilities

Current situation: Each system physically separated, system responsibility at the supplier.	 SW-1 HW-1 SW-2 HW-2 SW-3 HW abstraction HW-3 SW-4 HW abstraction HW-4
Step-1: Systems running on same hardware, system responsibility at the supplier; co-ordination of certification and safety assessment of the software-based systems needed	 SW-1 SW-2 HW abstraction HW-1 SW-3 SW-4 HW abstraction HW-2
Step-2: Systems of one supplier running on same hardware. Supplier provides only FS Software. Hardware and hardware abstraction are COTS, chosen, assembled and operated by a third party (computing platform operator). Certification and safety assessment for the software-based systems are separated from the computing platform, with responsibility either by: • The Supplier of the software-based system, contractually binding the operator of the computing environment OR	 SW-1 SW-2 HW abstraction HW-1 SW-3 SW-4 HW abstraction HW-2

• The RU/IM, contractually binding the operator of the computing environment to the safety management system. Overall responsibility with IM/RU	
Step-3: Systems of mixed suppliers running on same hardware. Supplier provides Functional System Software. Hardware and hardware abstraction software are COTS, chosen, assembled and operated by a third party (computing platform operator). Certification and safety assessment for the software-based systems are separated from the computing platform. Responsibility for the computing environment with the RU/IM, contractually binding the operator of the computing environment to the safety management system. Overall responsibility with RU/IM	
Step-4 (trackside only): Systems of mixed suppliers and mixed IM/RU running on same hardware. Suppliers provide Functional System Software. Hardware and hardware abstraction software are COTS, chosen, assembled and operated by a third party (computing platform operator). Certification and safety assessment for the software-based systems are separated from the computing platform. Responsibility for the computing environment with the computing platform operator, contractually related to the different IM and their safety management systems. Overall responsibility with IM down to their SMS and the need to contractually bind the computing platform operator. Independent authorisation of the computing platform operator by a neutral body.	 SW-1 SW-2 SW-3 SW-4 SW-1 SW-2 SW-3 SW-4 HW abstraction HW

6 ANALYSIS

The view on the current railway system, as described in Chapter 4, defines railway fixed and mobile system elements (network and vehicles) and subsystems (functional and structural ones) and sets out the rules to build and integrate the railway system in such a way that the involved subsystems and elements are interoperable and build up a performant railway system. As far as possible, the focus is restricted to interoperability, safety is covered as well but with less focus on the structure of the railway system.

TSIs are defined to cover the given subsystems. For the MPC, mainly the TSI CCS (covering trackside command-control and signalling as well as onboard command-control and signalling) is relevant and to a certain extent the TSI LOC&PAS (covering locomotives and passenger rolling stock).

Based on this, the following categorisation applies; a software-based component of the railway system is:

- subject to certification for interoperability if it implements functions specified by a TSI
- subject to safety assessment if it implements safety related functions

(possibly both).

If a software-based system does not implement a function specified by a TSI and does not implement a safety related function, then there is no need (with respect to the documents considered here) for respecting regulatory constraints; the aim for an MCP is to be separated well enough from the Functional Systems that it can be considered to meet this last condition.

As we have seen in chapter 5, separation of the Functional System Software and the Computing Environment appears feasible today, both with respect to interoperability and with respect to safety, if certain considerations are respected.

6.1 High Level Analysis and System Context

This section illustrates the need for adaptations to the current set of European Directives, Regulations and Standards, from general observations related to the MPC down to the detailed needs of leveraging the potential of the MPC in Railways.

6.1.1 Scope and integration paradigm of the current TSI CCS vs. the MPC

The TSI CCS details the structure of the CCS subsystem and the provisions for integration. The current TSI is based on the paradigm that integration can be done along a hierarchical tree structure, where accountabilities are exclusive and the control over alterations of components are broken down to the leaves of the tree vertically.

The following Figure 3 provides an example for the CCS Trackside subsystem breakdown. This figure thus illustrates the current European legislative framework relevant to the certification and authorisation and sets it into context to the MPC. It reflects the interaction between the overarching interoperability and safety regulations (notably Regulation (EU) 2016/797 and Regulation (EU) 2016/798), the applicable TSI (notably Regulation (EU) 2023/1695), and supporting guidance issued by the European Union Agency for Railways (ERA). The figure provides context for how CCS subsystems are currently assessed and authorised within the existing regulatory environment. In this current approach, each Functional System gets executed on its own specific infrastructure, resulting in inefficiency and lack of harmonisation. Concerning the trackside infrastructure, only RBCs are subject to certification along the current TSI subsystem break down, while interlockings, operation control centre software and traffic management software are affected by the safety related aspects of authorisation only.

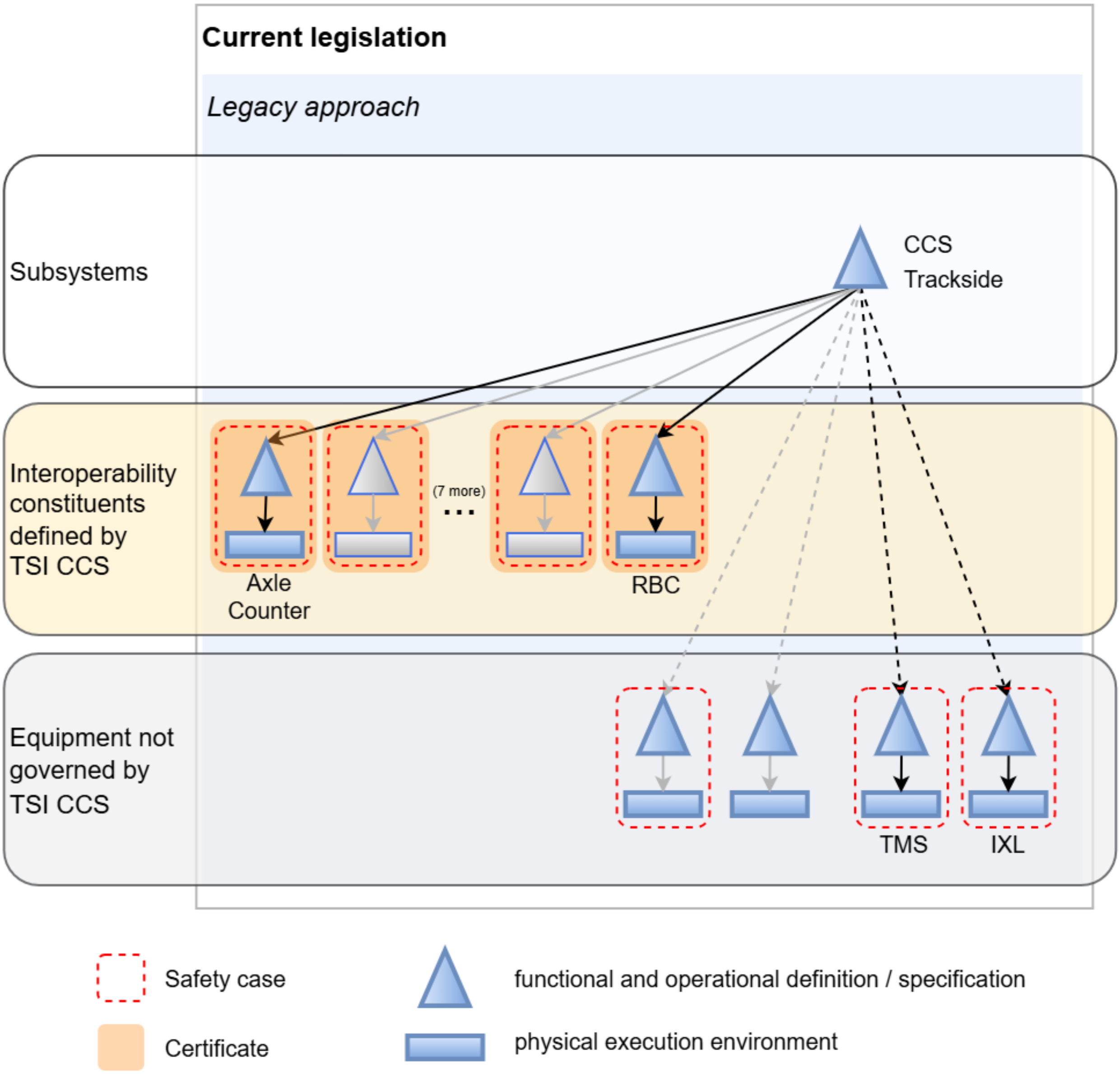

Current legislation
Legacy approach
Subsystems
CCS
Trackside
Interoperability constituents defined by TSI CCS
Axle Counter
(7 more)
...
RBC
Equipment not governed by TSI CCS
TMS
IXL
Safety case
Certificate
functional and operational definition / specification
physical execution environment

Figure 3: CCS Trackside Subsystem structured from the Perspective of current Directives and Regulations

For the Modular Platform Concept, this paradigm does not work due to its layered architecture. A Modular Computing Platform expectably supports software components of more than one integration branch of a hierarchical tree structure. This is visualised in Figure 4. The figure highlights that a transition from the current legislative framework towards future regulatory concepts enabling Modular Platform approaches, is necessary. It indicates how existing interoperability, safety, and authorisation processes do not support the intended multivendor approach for software in terms of certification. The figure complements the discussion on regulatory adaptation and evolution presented in this chapter.

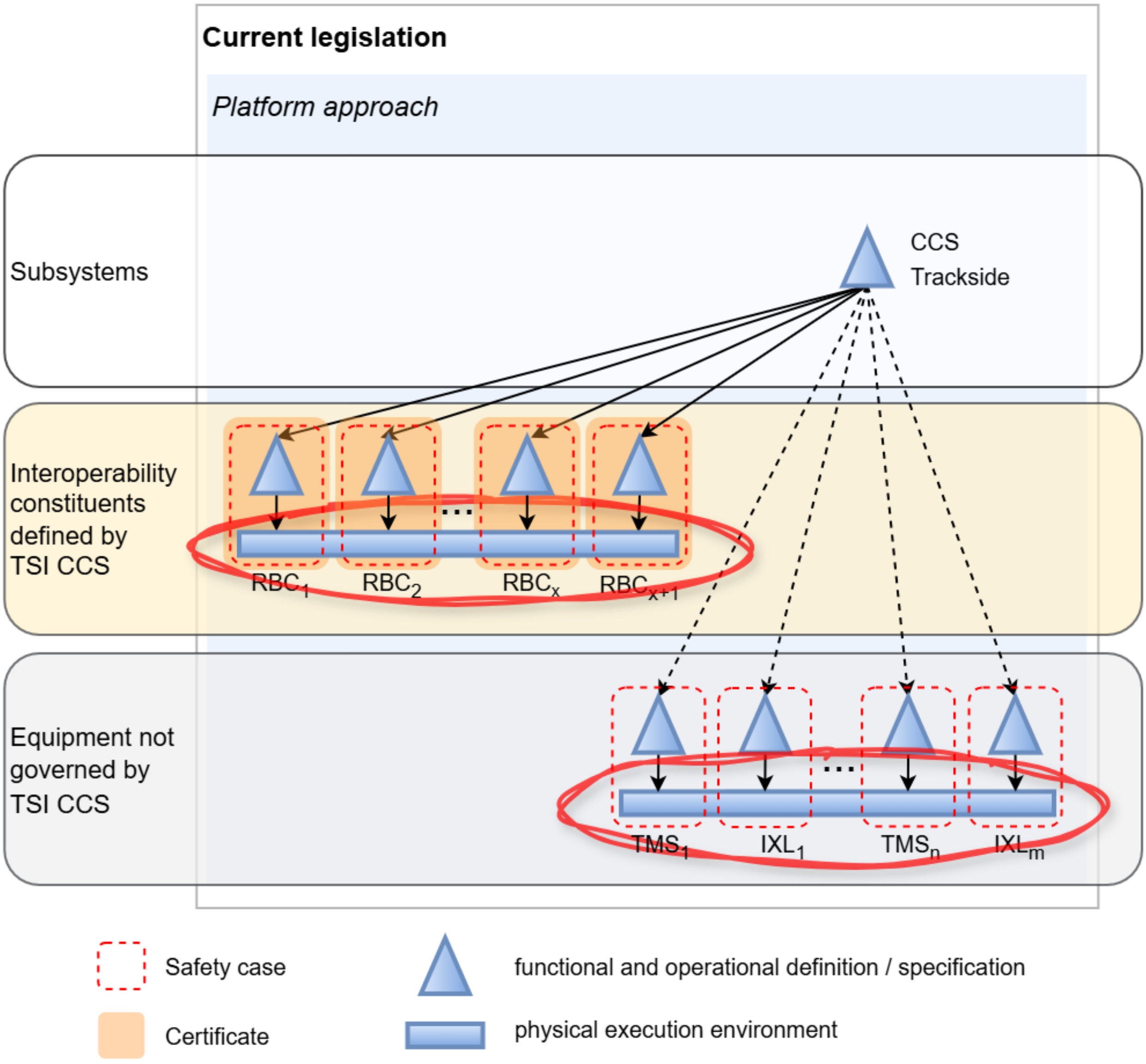

Current legislation
Platform approach
Subsystems
CCS
Trackside
Interoperability constituents defined by TSI CCS
RBC$_1$
RBC$_2$
RBC$_x$
RBC$_{x+1}$
Equipment not governed by TSI CCS
TMS$_1$
IXL$_1$
TMS$_n$
IXL$_m$
Safety case
Certificate
functional and operational definition / specification
physical execution environment

Figure 4: CCS Trackside Subsystem introcing a shared MCP

MCP Compartment Execution Environments, hosting several Functional Systems of multiple suppliers, reaching across the borders of different safety cases and certificates. Particularly if different stakeholders are responsible for the documents, this is currently a major obstacle for such a deployment.

Independently of the Modular Platform Concept, a general need to update the TSIs and/or the related regulatory documents, particularly TSI CCS, comes with the results of the System Pillar. To mention just one aspect of this, up to now the TSIs are clearly focused on interoperability aspects. With the new harmonised System Pillar reference architecture the entire CCS is covered, beyond the immediate necessities of interoperability. This should be reflected by the respective European directives and regulations. Doing this necessary update, the aspects relating to an adequate use of the MPC must not be kept out of scope.

Finding-1 With the new reference architecture of CCS/CCS+ in the System Pillar, it is foreseeable that the scope of the TSI CCS will be aligned with that new reference architecture. In that case, all the building blocks of the CCS subsystem presumably will be subject to the provisions of the TSI. This offers the chance respecting the topics brought up in this Deliverable D26.4 to an updated TSI, respecting necessary migration paths for existing products and installations.

6.1.2 Un-bundling software-based Systems from their physical Execution Environment

For many software-based systems the intended functionality is solely on the logical level, having data as input and data as output without physical functions to be executed. In the Modular Platform Concept, such data-only, software-based systems have been introduced as ‘Functional Systems’, a term used further in relation to such products.

As we have already seen in the analysis of the current TSI CCS in section 6.1.1, certification and authorisation of Functional Systems along the currently given provisions is inefficient (by executing unnecessary controls) and impairs evolution of the railway system; this goes beyond the TSI CCS.

The current approach establishes trust in the deployed technical equipment by defining and controlling their logical and physical implementation together, assembling the equipment into the overall railway system by integrating them level by level in a hierarchical tree structure, following the concept of safe integration.

For Functional Systems, the necessary depth of analysis with respect to the physical implementation can be reduced substantially. Already today, with the use of adequate safety layers in the logical part, safety cases for Functional Systems are separated from the computing platform. Even the use of COTS components can be authorised and often is. Yet still, the version and configuration of the computing platform is an integral part of the documented system under consideration for the certification, and for the authorisation to be operated as part of the railway system.

To leverage the potential of modern IT/OT operation, this needs to be un-bundled as far as possible, most of all in terms of safety functions (which can and should be kept within the logical part, as long as data is the input as well as the output of a system), and the paradigm of a hierarchical tree structure needs to be abandoned allowing the operation of multiple Functional Systems on one computing infrastructure.

To reach this goal, the MCP technically needs to be properly separated from the Functional Systems executed on the MCP (as mentioned, this is already demonstrated to be possible by some products in the sector). This is covered by the SP and R2DATO activities concerning the Modular Platform

Concept, resulting in technical requirements towards the Modular Computing Platform such that the MCP can be conformity-tested against them, including any necessary Safety Related Application Conditions (if unavoidable).

Furthermore, the MCP must be operated by an organisation staffed with skilled and properly instructed personnel, to make sure that along the entire life cycle of a specific MCP the necessary conditions to execute the Functional Systems safely is always given. This organisation needs to implement and follow the required processes related to the operation and the lifecycle in general of the MCP, to ensure adequate maintenance and evolution of the specific MCP. This includes the provisions set out by the SP PRAMS evolution management process [13]. We will come to that in more detail in section 6.1.4

Both aspects (interface specification and organisational setup), already today, could be implemented on a system-by-system basis by technical specifications (addressing the manufacturers) and binding contracts (addressing the organisations operating specific MCPs).

They could be bound contractually and integrated into the SMS of the respective IM/RU. If such contracts can be set up without collisions, it would even be possible that on a specific MCP, Functional Systems for different IMs is executed) but getting prohibitively complicated as soon as several manufacturers and IMs get involved.

Figure 5 illustrates the potential future legislation in the course of a harmonised CCS Reference Architecture, introducing and implementing the MPC.

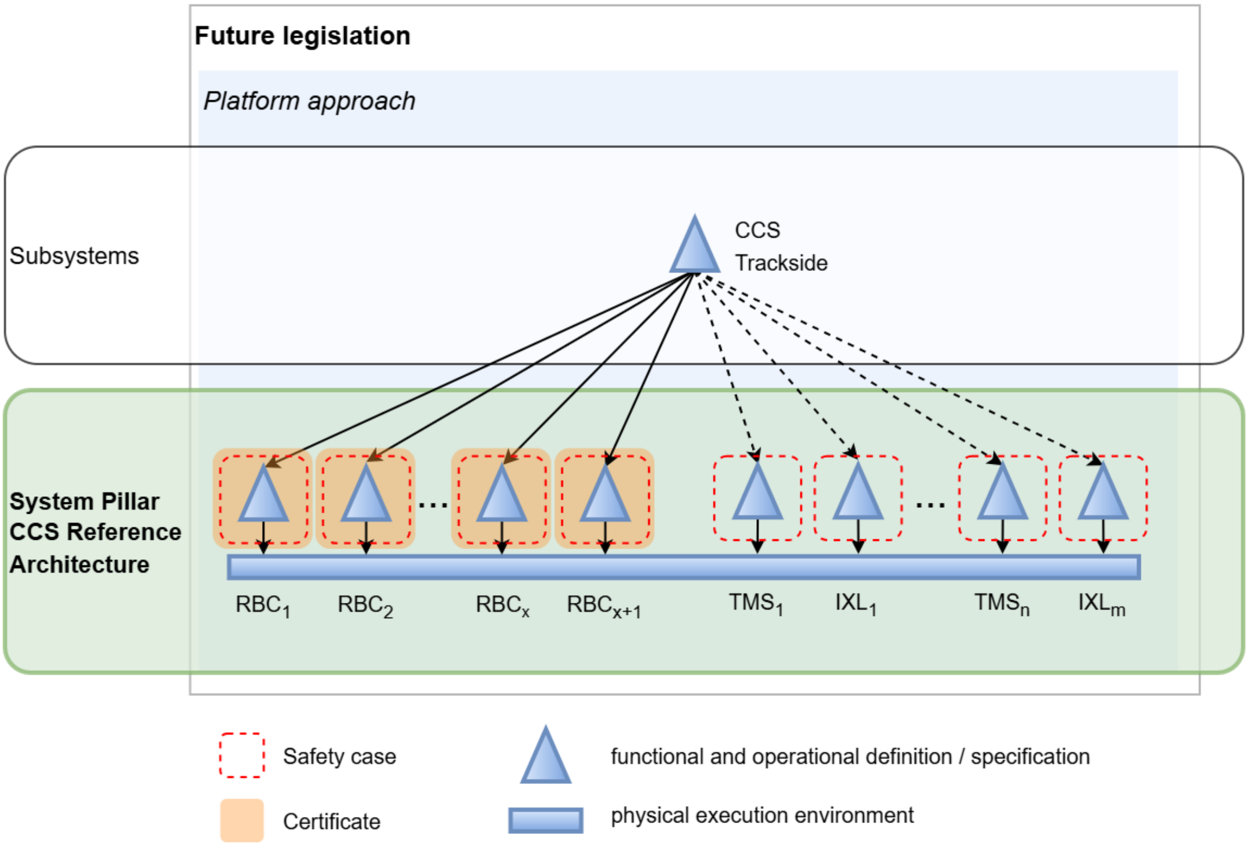


Figure 5: Potential Future Legislation in the Course of the MPC

It presents the legislative perspective for Modular Platform certificates, illustrating safety cases being restricted to the hosted functional systems and raising the need to apply common assessment principles, and trust-based certification approaches. It reflects how a more integrated and modular friendly regulatory framework could support lifecycle and change management, and cross-project reuse of certified subsystems deployed on the MCP.

Finding-2 To leverage the full potential of co-locating software-based systems, harmonised technical specifications need to be established for the interfaces of the MCP towards the Functional Systems (among others, in line with the upcoming SP CE I3 specification), such that MCPs can qualify against them.

It must be noted that such specifications are only furthering the situation if they are kept as simple and concise as possible. In particular, the safety relevant aspect must be minimised, best avoided (and this seems possible at least in the near future, based on the previous work in System Pillar and Innovation Pillar. Currently, there are some remaining safety related aspects in the MPC, namely the NHA).

Finding-3 As technology moves on quickly in the IT sector, these specifications for Compute Platforms will have their best effect if they are administered by a body independent from individual actors in the sector, being able to react on developments and circumstances in the time scale of the technical domain.

6.1.3 Deployment Scenarios and Involved Actors

As soon as the physical equipment is properly un-coupled from the software in a harmonised way as described in section 6.1.2, the doors are open to actively support the desired benefits expected from the Modular Platform Concept by frameworks for certification and authorisation.

The feasibility of operating multiple Functional Systems, possibly of different manufacturers, on one installation of a Modular Computing Platform is strongly related to how accountabilities are arranged between the different actors. The different obvious options for un-bundling interdependencies are illustrated by Table 4. To leverage the full potential, accountabilities need to be rearranged in a way reflecting the deployment structures one desires to support and encourage, and the processes governing certification and authorisation need to reflect this as well.

As we have worked out in sections 6.1.1 and 6.1.2, deployment structures involving multiple Functional Systems on one MCP necessitate a new trust model where manufacturers of Functional Systems are allowed to rely on general purpose computing functionality based on standardised interfaces, to be provided sufficiently well and documented independently from the Functional Systems themselves.

Deployment structures involving one or several of the following aspects:

- Functional Systems of multiple manufacturers running on one MCP
- Functional Systems relating to different contexts of safe integration (e.g. RBCs not belonging to the same line) running on one MCP
- Functional Systems of multiple IMs running on one MCP

are only possible if the hierarchical tree paradigm is dropped. As the bullet list implies, an important aspect in abandoning the hierarchical tree paradigm is, whether this shall be viable only within one network area of use or even across network areas, or whether even different infrastructure managers may share MCP resources. For on-board, this situation is simpler, as sharing computing resources always happens under the same RU responsible and within the same safe integration context.

In its most advanced variant, this supports Functional Systems of different manufacturers providing functions for different IMs to be executed on shared computing infrastructure offered by another actor.

Today, such an 'outside' actor providing and operating computing infrastructure could be involved by contractual obligation and integration into the Safety Management System of an Infrastructure Manager or a Railway Undertaking; but this would neither be harmonised nor would services be offered towards several IMs/RUs be covered. Moreover, it would seem a bad allocation of responsibilities when the railways have to take contractual control over integration and documentation while they do not have the technical expertise for those systems.

Finding-4 To adapt processes of certification and authorisation for best leverage of the Modular Platform Concept, a decision has to be taken which variants (please refer to Table 4: Possible Options for Deployment Structures and Responsibilities) should be explicitly supported by the legal framework:

- Shall an MCP instance be used by Functional Systems of one manufacturer only or shall it be supported that Functional Systems of different manufacturers share MCP resources?
- Shall an MCP instance be used by one IM/RU only or shall it be supported that different IM/RUs share MCP resources?

This is a necessary prerequisite for defining processes, obligations and actors adequately.

Finding-5 To leverage the full potential of the Modular Platform Concept, accountabilities and obligations around the operation of Modular Computing Platforms and their lifecycle need to be attributed to the actors in a defined and harmonised way. To ensure an efficient, scalable and feasible implementation, it appears most promising to define a new actor (who is in charge of operating the Modular Computing Platforms) in the legal framework (vaguely comparable to the Entities in Charge of Maintenance). Please compare as well Finding-6.

6.1.4 Maintenance and System Evolution

An MCP instance can be qualified to conform to harmonised requirements upon or before its installation; yet this doesn't cover the life cycle of the overall system or the MCP instance itself adequately. Both, the Functional Systems executed on an MCP as well as the MCP itself, will be subject to maintenance and evolution.

The frequency of needed changes will rise compared to today not only due to technological change of computing infrastructure and from the rising OT security needs in general, but just as much from the increasing integration and automation of the railway system, namely, the effects the System Pillar reference architecture implies on maintenance and system evolution: The integration of individual technical systems of the railway system into a system of systems makes changes affect other systems and induces 'lack of movement' as a driver for unexpected system behaviour and malfunctions. This will incur constant evolution to cope with the changing environment.

All of this makes it obvious that the legal framework in the future must be designed to allow for constant evolution of software-based railway systems and their computing resources, rather than sticking to the 20th century 'certify-once-then-run-for-a-lifetime' approach. A lot has been achieved in that respect in the latest versions of the respective European Directives and Regulations, nonetheless, maintenance and evolution with focus on the interface between Functional Systems and MCPs as well as maintenance and evolution of the MCPs themselves under the responsibility of an independent actor is a new aspect brought into the field by the SP and R2DATO efforts on the Modular Platform Concept.

Analysis shows easily that with respect to the evolution of the Functional System, the MCP needs to 'only' support the functionality enabling maintenance and evolution of the Functional System. Change and (re-)certification of a Functional System shall be applicable without impact on other Functional Systems executed on the same MCP, as far as possible. These aspects can be made part of the MCP requirements such that an MCP can be qualified against it.

Concerning the lifecycle of the MCP itself, there is a number of aspects to take care of to enable the safe execution of the hosted Functional Systems:

- The MCP must be operated by an organisation staffed with skilled and properly instructed personnel, to make sure that along the entire life cycle of a specific MCP, the necessary conditions to execute the Functional Systems safely are respected at all times.
- The organisation operating the MCP needs to implement and follow the required processes related to the operation and the lifecycle of the MCP in general, to ensure adequate maintenance and evolution of the specific MCP, including configuration management (e.g., for CEME) and software updates (change or security patches) for the platform management.
- The required processes related to the operation and the overall lifecycle of the MCP (e.g. which kind of alterations are appropriate, to be performed by whom, accounted for by whom, to be documented by whom and where) need to be defined (with the adequate level of abstraction) in a harmonised way together with the harmonised technical specifications for the MCP (please compare Finding-2 and Finding-3 and for the options of the desired deployment structure please compare Finding-4). This relates in particular to the provisions set out by the SP PRAMS evolution management process.

Finding-6 To leverage the full potential of the Modular Platform Concept, the accountabilities, responsibilities, obligations and basic capabilities of service providers operating Modular Computing Platforms need to be defined in a harmonised way, in particular reflecting the provisions set out by the SP PRAMS evolution management process.

6.2 Analysis Regarding Cybersecurity

For integrated systems security must be ensured as well as safety. This applies to all parts of the MPC, including the communication towards the Shared Services (please refer to Figure 2: High Level MPC Service Architecture). Since all other sections are handling the safety aspects and resulting obligations, a separate analysis concerning the integration of security in the foreseen systems approach is presented here.

To guide the security approach particularly the publications listed in 4.5.4, the IEC 62443 standard series for integrating IT and OT security and the IEC 63452 standard are relevant. IEC 63452 is currently in review and adopts the IEC 62443 series for the railway industry.

In integrated systems, the topics defined by these standards need to be addressed. However, due to the integrated nature of such a system, where several actors are responsible for different integrated software components on the same servers, a special focus needs to be put on:

- Ensuring clear boundaries for the responsibilities of the actors,
- Define interfaces between the actors, e.g. for triggering maintenance actions, and
- Define obligations for the actors to ensure an overall secure system.

Unlike in today's safe systems where everything is under control of one actor, the response time of all the involved actors and their interactions may be crucial. Furthermore, safety relevant software may not be updated as quickly as non-safe software. Therefore, the zoning concept as defined in IEC 62443 needs to be defined for the integrated system from the start, too.

The following two scenarios highlight the importance of well-defined interfaces between the involved actors and their timely actions:

Scenario 1: Regular patch management

Regular updates need to be performed due to security findings such as Common Vulnerabilities and Exposures. The focus of the individual update is one of the following two levels:

- Virtual machine level: every change that is part of the virtual machines and the contained application and operating system software.
- Hardware abstraction level: every change that is part of the hypervisor, the operating system and the server firmware.

These updates must be regularly performed. Each actor must provide the information on when such updates need to happen and clear protocols for managing these updates need to be established.

Scenario 2: Zero-day vulnerability

Zero-day vulnerabilities, i.e. vulnerabilities that are already exploited, may need to be handled separately from the regular patch management. A dedicated group of people nominated by all actors might need to work together to identify the appropriate response. It needs be clearly defined which actors monitor these vulnerabilities and then subsequently trigger such a response team. Also, the processes for the response team need to be specified.

Finding-7 The scenarios presented highlight the need for a comprehensive security strategy for the integrated system. This strategy should clearly define all involved actors, their responsibilities, and the interfaces between them to ensure safe and secure operation. The SP PRAMS domain is currently developing requirements and processes aimed at decoupling cyber-security-related changes from safety-related changes, thereby enabling faster and more frequent system updates. To support this effort, the current document should be shared with the SP PRAMS domain to ensure that the modular platform case is appropriately considered. The SP PRAMS domain may explicitly consider the discussions related to modular certification boundaries, interface standardisation, responsibility allocation between system integrators and component suppliers, and the reuse of certification evidence across different platform configurations. In particular, evolution aspects such as change and configuration management, and the treatment of safety and cybersecurity requirements at component level are of direct relevance and will be reflected in future SP PRAMS activities. A first vision of the certification boundaries, responsibility allocation can be found in Appendix B in this document.

7 RECOMMENDATIONS

This chapter summarises the main results of the conducted work providing concrete recommendations. Unsolved challenges and open points are presented in 8.3 of the final Conclusion chapter.

Recommendation-1

As, in the wake of the new harmonised reference architecture of the System Pillar, an update of at least the TSI CCS seems hard to avoid (to include the additional building blocks of the CCS subsystem). This foreseeable update should take into account the findings and recommendations of this Deliverable D26.4, where concepts described in Chapters 4, 5, and 6 specify certification boundaries, applicable assessment methods, and the reuse of certification evidence. It must be ensured that the approaches are well represented and maintained in the Standardisation and TSI Input, planned and further driven by the accountable parties.

Recommendation-2

To leverage the economic potential of MCPs, the requirements of Functional Systems towards MCPs need to be harmonised and provided in a way so that MCPs can efficiently be tested for compliance. This requires early coordination between manufacturers, system integrators, and assessment bodies to ensure that cost optimisation does not compromise safety, interoperability, or regulatory compliance, as discussed in Sections 5 and 6. This harmonised approach also implies the need to evaluate whether these technical specifications should be included into the TSI CCS or whether a setup outside the TSI is preferable, comparable to the vehicle type registers. Important to note here that if ever possible, there should be only one such specified profile for an MCP at a time; yet, differing requirements between on-board and trackside as well as the expected support for migration and evolution paths will lead to at least a small number of MCP profiles in parallel, with differing specifications.

Recommendation-3

The profiles for MCPs referred to in Recommendation-2 will have their best effect if they are administered by a body independent from individual actors in the sector and able to react on developments and circumstances in the time scale of the technical domain. This implies the need to evaluate how a body governing the MCP specification(s) could be formed most easily and effectively (finding the adequate sourcing of technological and regulatory prowess for that body within the sector) and what would be the best way to introduce it, be it in European Directives or Regulations or in the TSI CCS.

Recommendation-4

The introduction of the Modular Platform Concept requires a sector-wide evaluation of which deployment structures should be supported and promoted, as outlined in Recommendation-3, it is recommended to analyse potential implications for the definition of roles, responsibilities, and accountabilities within the European railway regulatory framework. An explicit decision on this matter is necessary. Table 4: Possible Options for Deployment Structures and Responsibilities, illustrates the varying degrees of unbundling and interdependencies. This table serves as a foundation for any necessary adaptations to the legal framework in support of the Modular Platform Concept. The outcome of the before mentioned evaluation is essential for understanding potential implications for certification, authorisation, and regulatory alignment, as discussed in Chapter 6.

Recommendation-5

The choice of which MCP deployment structures shall be supported, as outlined in Recommendation-3, creates a need to review and adapt the European railway Directives and Regulations that defines system actors and their responsibilities. It must be clarified which requirements an organisation has to fulfil to manage the lifecycle of an MCP installation and to operate functional systems on it. A straightforward approach would be adding a new actor in the European Directives and Regulations for the MCP, similar in concept to the Entities in Charge of Maintenance.

Recommendation-6

If the Modular Platform Concept is applied consequently, the life cycles of an MCP and of the Functional Systems executed on it are uncoupled and expectedly feature a higher frequency of changes compared to existing railway equipment. This is referred to by Sections 6.1 and 6.2, where the decoupling is explained in detail. The process is thus leading potentially to increased frequency of changes. This implies the need to define the provisions governing the life cycle of the MCP and its support for the life cycles of the Functional Systems with special care. An adequate way to have these provisions established in a harmonised way needs to be evaluated. This relates in particular to the provisions set out by the SP PRAMS evolution management process.

Recommendation-7

The analysis in Section 6.2 highlights that the application of modular platforms introduces specific cybersecurity challenges related to the allocation of responsibilities and the definition of interfaces between actors. The challenges concerning cybersecurity need to be addressed, in particular the precise definition of actors, their responsibilities, and interfaces between the actors need to be performed. It is recommended that these aspects get further examined in the context of the existing cybersecurity framework of the System Pillar and further work within R&I projects. One obvious way would be to address the identified cybersecurity challenges to the SP PRAMS domain considering the Modular Platform case as well.

Recommendation-8

The potential use of centralised approaches in modular platform architectures, as discussed in Chapter 6, may introduce specific resilience and availability challenges. It is recommended to analyse and assess these challenges systematically in future activities of ERJU and to explore suitable mitigation strategies, such as geo-redundancy or distributed solutions, in alignment with safety, security, and availability considerations defined in the regulatory framework.

8 CONCLUSION

The work carried out in Task 26.3 has successfully addressed its objectives resulting in the provision of this deliverable, providing a comprehensive analysis and set of recommendations for the certification and homologation of Modular Computing Platforms (MCPs) within the European railway system. This deliverable builds upon previous efforts in WP26 and aligns closely with Europe's Rail System Pillar, particularly in the domains of Computing Environment, PRAMS, Transversal CCS, and Cybersecurity.

8.1 Achievements and Contributions

The study has achieved the following key outcomes:

- **Regulatory Landscape Analysis:** A detailed mapping of the current European directives, regulations, and standards relevant to MCP certification was conducted. This revealed structural limitations in the existing framework, particularly its reliance on vertically integrated, hardware-bound certification models.
- **Modular Platform Concept (MPC):** The deliverable elaborated on the MPC architecture, emphasizing the separation of functional systems from their physical execution environments. This decoupling is essential for enabling scalable, cost-effective deployment and maintenance of software-based railway systems.
- **Role and Responsibility Definition:** A trust model was proposed, identifying new roles and responsibilities for stakeholders involved in MCP certification. This includes the potential introduction of a new actor akin to the "Entity in Charge of Maintenance" and lifecycle management for MCP.
- **Cybersecurity Integration:** The work highlighted the need for harmonised cybersecurity processes, especially in multi-actor environments. Scenarios such as zero-day vulnerabilities and patch management were analysed to demonstrate the importance of coordinated response mechanisms.
- **Recommendations for TSI Evolution:** The deliverable recommends extending the scope of Technical Specifications for Interoperability (TSIs) beyond interoperability to include horizontal integration, modularity, and lifecycle management. This is crucial for aligning with the System Pillar's reference architecture and supporting MCP deployment.

8.2 Evaluation and Lessons Learned

The work has demonstrated that while the current regulatory framework provides a solid foundation, it lacks the flexibility required for modular, software-based systems which feature no physical functionality. Key challenges encountered include:

- **Fragmentation of Certification Processes:** The existing hierarchical certification model impedes the co-location of functional systems from multiple suppliers on shared infrastructure.
- **A current lack of Harmonised MCP Solutions:** Without standardised MCP specifications, certification remains vendor-specific and inefficient.

- **Slow Regulatory Adaptation:** The pace of regulatory change does not match the rapid evolution of IT/OT technologies, posing a risk to innovation uptake.

Despite these challenges, the task has laid the groundwork for a more agile and modular certification approach, aligning with the strategic goals of Europe's Rail.

8.3 Open Points

Based on the Recommendations from Chapter 7 further important Open Points are:

Open-1 Relevant specifications of the SP CE, PRAMS and Transversal domains need to be further developed, finalised and published. Further demonstration of the MPC in the context of standardisation and future R&I projects will be decisive to enable fully operational deployments in real environments.

Open-2 Generally, the Railway Sector is facing a very slow progress implementing safety-related topics (e.g., additions to future TSIs). The technical standardisation is currently driven in ERJU SP, but adaptions and further establishments of technical and legal topics may take longer than the SP is planned to be mandated.

Open-3 The definition and formalisation of the proposed new actor for MCP operation and maintenance in future TSIs and European Directives and Regulations will be pivotal.

Open-4 A clarification of deployment options that need to be supported (e.g., multi-vendor and/or multi-IM/RU MCPs) must be achieved in the future.

Open-5 Integration of cybersecurity specifications into future TSIs.

Open-6 On-board specific considerations require further study since they could not be considered in detail during the analysis of this deliverable. This might induce additional aspects or may result in other specific conflicts with existing regulations.

8.4 Proposals for Further Activities

To ensure continuity and impact, the following actions are proposed:

- **Standardisation Input:** Ensure findings are represented in the STIP and future TSI updates beyond interoperability topics, integrating the needs of horizontal integration towards subsystems. MCP technical and organisationally interests must be reflected and considered by future TSIs, eventually introduce needed adaptions in European Directives and Regulations.
- **On-board Subsystem Analysis:** Extend the study to cover on-board MCP applications.
- **Pilot Implementations:** Support high-TRL demonstration projects to validate the proposed trust model and certification workflows.
- **Cross-domain Collaboration:** Strengthen ties between SP domains to harmonise safety, cybersecurity, interoperability and interchangeability requirements in a harmonised Modular Railway System Architecture.

REFERENCES

[1] The Europe’s Rail Mission and Objectives
https://rail-research.europa.eu/about-europes-rail/europes-rail-mission-and-objectives/

[2] ERJU System Pillar – Common Business Objectives
https://rail-research.europa.eu/wp-content/uploads/2022/10/SP-Common-Business-Objectives.pdf

[3] ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.1
“High level Consolidation”
https://rail-research.europa.eu/pages/fp2-r2dato/deliverables

[4] ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.2
“Intermediate specification of the Modular Platform”
https://rail-research.europa.eu/pages/fp2-r2dato/deliverables

[5] ERJU Innovation Pillar FP2 R2DATO, Work Package 26, Deliverable D26.3
“Final Modular Platform requirements, architecture and specification”
https://projects.rail-research.europa.eu/eurail-fp2/deliverables/

[6] Computing Platform – Whitepaper:
https://github.com/OCORA-Public/Publications/blob/master/00_OCORA%20Latest%20Publications/Latest%20Release/OCORA-TWS03-010_Computing-Platform-Whitepaper.pdf

[7] Computing Platform – Requirements:
https://github.com/OCORA-Public/Publications/blob/master/00_OCORA%20Latest%20Publications/Latest%20Release/OCORA-TWS03-020_Computing-Platform-Requirements.pdf

[8] Computing Platform – Specification of the PI API between Application and Platform:
https://github.com/OCORA-Public/Publications/blob/master/00_OCORA%20Latest%20Publications/Latest%20Release/OCORA-TWS03-030_SCP_Specification_of_the_PI_API_between_Application_and_Platform.pdf

[9] ERJU System Pillar, Computing Environment – Deliverable “Recommendation on interfaces to be standardised”
Document list: https://rail-research.europa.eu/task-2-ccs/
Document access: *not yet publicly available*

[10] ERJU System Pillar, Computing Environment – Deliverable “System Concept including Operational Analysis” (the old title was used in this deliverable: “Operational Analysis Specification”)
Document list: https://rail-research.europa.eu/task-2-ccs/
Document access: *not yet publicly available*

[11] ERJU System Pillar, Computing Environment – Deliverable “System Analysis “
Document list: https://rail-research.europa.eu/task-2-ccs/
Document access: *not yet publicly available*

[12] ERJU System Pillar, Cybersecurity Specifications Document list: https://rail-research.europa.eu/horizontal-tasks/
Document access: https://rail-research.europa.eu/wp-content/uploads/2025/03/ERJU-SP-Cybersecurity-Specifications-V1.0.zip

[13] ERJU System Pillar, Evolution management of safety-related modular systems - Process and organisation: https://rail-research.europa.eu/system_pillar/draft-documents/
Document access: https://rail-research.europa.eu/wp-content/uploads/2025/06/PRAMS.zip

[14] ERJU System Pillar, Safety Case - Strategy for Generic Design Safety Cases: https://rail-research.europa.eu/horizontal-tasks/
Document access: *not yet publicly available*

[15] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety: https://eur-lex.europa.eu/eli/dir/2016/798/oj/eng

[16] 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: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0797&qid=1756992772052

[17] Common Safety Methods on Safety Management System Requirements: https://www.era.europa.eu/domains/common-safety-methods/safety-management-system-requirements-csm_en

[18] NIS 2 (Directive (EU) 2022/2555): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1756992187529

[19] Cyber Resilience Act (Regulation (EU) 2024/2847): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1756992545747

Appendix

APPENDIX A

This Appendix provides a general overview of the European regulatory landscape, the relevant directives, regulations, standards and guidelines, their hierarchy and binding force.

Some historical background on the railway system before and after the introduction of ETCS

In conventional rail systems of the 20th century, both design and operation were defined on a national level. The interaction between rolling stock and infrastructure was primarily physical: gauge, radius of turns, platform height and length, voltage, and height of catenary defined the compatibility. These parameters were set by each country.

Safety and control relied on national ATP systems and cab radios each developed and managed by the infrastructure manager. This has led to more than twenty country specific solutions in Europe, with many regional operational rules and national authorisation procedures. As a result, rolling stock operating internationally needed to be fitted with multiple systems, and had to undergo separate national homologation processes. Certification and approval were carried out at national level, mostly by the infrastructure manager or National Safety Authority (NSA), with route-specific procedures.

High speed rail introduced more integrated train control (e.g. TVM in France and Belgium) but remained nationally defined and confined to specific lines. Cross border high speed operations, such as with Thalys PBKA units, required multi voltage traction and multiple signalling systems. Certification and approval processes stayed at the national level, usually route-specific and overseen by NSAs or infrastructure managers.

The European Train Control System (ETCS), as part of ERTMS, was developed to harmonise ATP and cab signalling across networks. While the focus remains on interoperability at the train track interface, the system includes a defined migration path from legacy “Class B” systems to a common European standard. Overall technical specifications, rules of operation and regulations concerning approval are centrally defined based on EU directives and regulation (DIRECTIVE (EU) 2016/798, Article 2, with a scope which is restricted to interoperability train-track). However, interoperability is only factually achieved in specific areas of use and still subject to restrictions at national level (with national values etc.).

This means that the ETCS implementation introduced a more centralized approval processes and allowed for responsibilities to be transferred from NSAs to ERA, where justified. Thus, the current harmonisation at European level, through the CCS TSI, addresses the safety and interoperability requirements, the on-board functions and the interfaces between trackside and on-board related to train protection, signalling the permission to move the train and radio communication. These developments have led to the European directive “Directive (EU) 2016/798, Article 2”**,** which establishes that the European rail system can be considered both as a whole and as a set of structural and functional subsystems. This breakdown is not only a technical classification it also shapes how assessments, certificates, and authorisations are applied in practice (System Level, Interoperability Level and Subsystem Level). Those are described in more detail in the following sections.

Introduction of Europe’s Rail Joint Undertaking (ERJU) to the landscape

With the introduction of the System Pillar under ERJU, the scope of harmonisation is expanding. The aim is to define the full functional architecture of the CCS system (CCS+), including interlockings and traffic management. This may require adaptation of current legislation and TSIs to reflect the target system architecture. The new proposed architecture will, to some extent, not match the current system breakdown.

In this context, certification remains an essential part, where a better alignment for systems can be provided, not only as a compliance process, but as a mechanism to structure responsibilities and align national systems with a shared European framework.

General overview

This section gives an overview of the legislation which is in place at the very moment, as well as standards and guidelines which were analysed.

The existing European regulatory framework for certification and authorisation of current systems and interoperability constituents in railways are derived from the following overview.

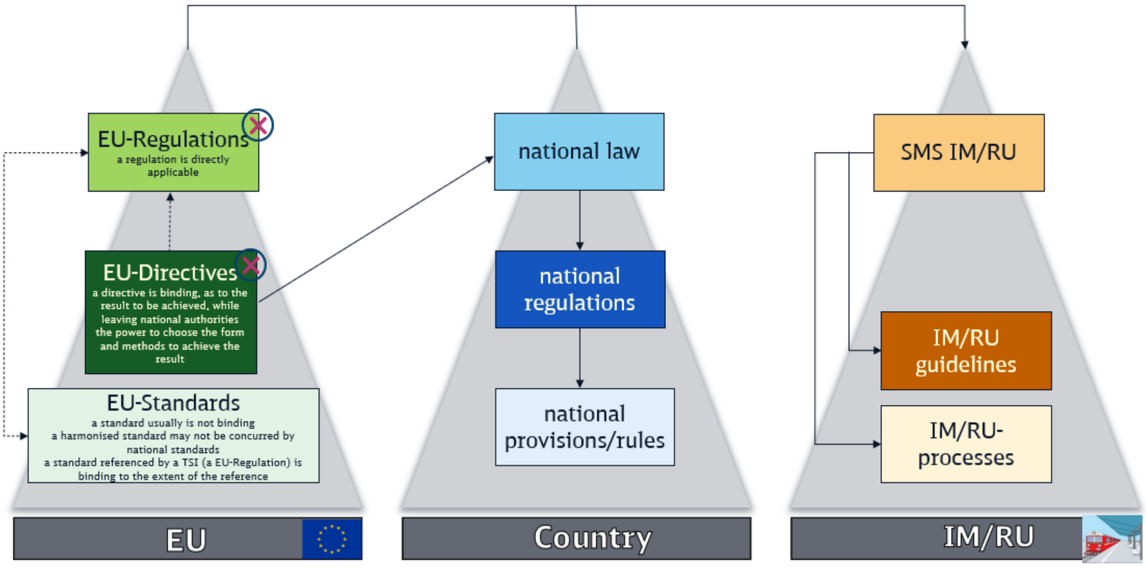

EU-Regulations
a regulation is directly applicable
EU-Directives
a directive is binding, as to the result to be achieved, while leaving national authorities the power to choose the form and methods to achieve the result
EU-Standards
a standard usually is not binding
a harmonised standard may not be concurred by national standards
a standard referenced by a TSI (a EU-Regulation) is binding to the extent of the reference
EU
national law
national regulations
national provisions/rules
Country
SMS IM/RU
IM/RU guidelines
IM/RU-processes
IM/RU

Figure 6: Hierarchy and Binding Force of various legal Documents at European (EU), National (Country), and IM/RU (Infrastructure Manager/Railway Undertaking) Levels

The regulatory landscape can be described through their binding force as well as where it originates:

On the European level the landscape can be described as follows:

- EU Regulation is directly applicable in all member states without needing national implementation. It is a law which is immediately enforceable.
- EU Directive is binding as to the result; this means member states must implement directives via national legislation. It is therefore a semi-hard law which creates obligation but allows flexibility in how goals are achieved on a national level.
- EU Standards are generally non-binding, unless referenced by a regulation or technical specification for interoperability (TSI). It could be described as a soft law and can thus become binding in specific contexts.

On a national level the following description is in place:

- National Law is directly applicable within a country and forms the highest level of enforceable rules. It is a law which is immediately enforceable by courts and state authorities.

- National Regulation is binding within the country and provides detailed rules to implement national laws. It is a hard law, enforceable and must be observed by all relevant parties within the jurisdiction.
- National Provisions/Rules are specific requirements and technical standards established based on national laws or regulations. These are enforceable legal obligations for defined scopes, considered hard law for those addressed.
- National Standards are usually not binding unless referenced by national law or regulation. They can be regarded as soft law, providing recommended practices or technical guidance, but they may become binding if explicitly required by a legal act.

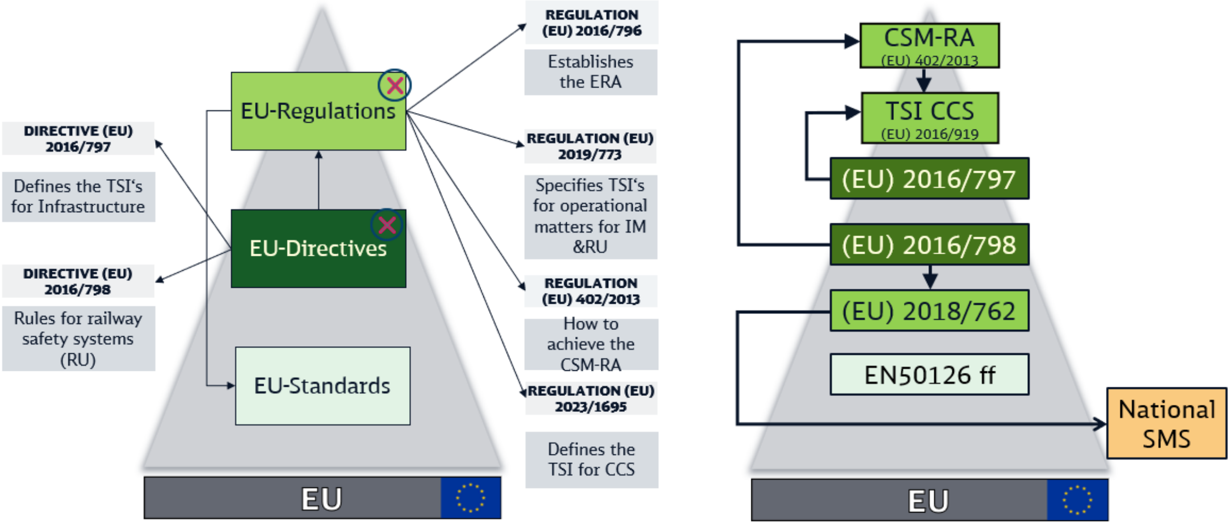


Figure 7: Directives, Regulations and Standards relevant for the Analysis

The following table provides an overview of Directives and Regulations used for the analysis.

Table 5: Overview of Directives and Regulations

Regulation / Directive	Short explanation
REGULATION (EU) 2016/796	*On the European Union Agency for Railways and repealing Regulation (EC) No 881/2004.* Establishes the European Union Agency for Railways (ERA) and outlines its responsibilities in ensuring safety and interoperability.
DIRECTIVE (EU) 2016/797	*On the interoperability of the rail system within the European Union.* Aims to ensure interoperability among national railway systems by setting out technical specifications and requirements. Specifies the TSI's for Infrastructure

Regulation / Directive	Short explanation
DIRECTIVE (EU) 2016/798	*On railway safety.* Focuses on enhancing railway safety across the EU by defining responsibilities and establishing a Single Safety Certificate. Defines rules for railway safety systems (RU)
REGULATION (EU) 2019/773	*On the technical specification for interoperability relating to the rail system in the European Union.* Addresses interoperability requirements for various railway components, including safety and operational aspects. Specifies the TSI's for operational matters for IM & RU
REGULATION (EU) 2023/1695	*On the technical specification for interoperability relating to the CCS subsystems of the rail system in the European Union.* Provides technical specifications for interoperability concerning CCS subsystems, replacing Regulation (EU) 2016/919. Defines the TSI for CCS
REGULATION (EU) 402/2013	*On the common safety method for risk evaluation and assessment and repealing Regulation.* Establishes a standardized risk management framework for assessing and mitigating risks associated with significant changes in the EU railway system, ensuring safety, harmonization, and interoperability across EU Member States. How to achieve the CSM-RA
REGULATION (EU) 2018/762	*Establishing common safety methods on safety management system requirements.* Establishes the CSM
REGULATION (EU) 2018/763	*Establishing practical arrangements for issuing single safety certificates to railway undertakings.* Provides the safety certificate definition
REGULATION (EU) 2018/545	*Establishing practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process.* Establishes vehicle authorisation processes
DIRECTIVE(EU) 2012/34	*Establishing a single European railway area.* Establishing SERA
RECOMMENDATION (EU) 2019/780	*On practical arrangements for issuing safety authorisations to infrastructure managers.* Defines how IM can manage authorisation

APPENDIX B

The following tables are presenting the actors that have been identified during the analysis, their responsibilities, relevant activities and main obligations in respect to certification and authorisation to Railway functions and subsystems hosted on the MCP. One detailed example, covering deployment, integration and maintenance scenarios of the MCP, gets presented in Appendix C.

Table 6: Main Obligations of Actors on System Level

System Level Actor	Main obligations in context with this deliverable
ERA	• Ensuring that railway safety is generally maintained and where reasonably practicable, continuously gets improved • draft the CSM • draft the CST (the minimum safety levels to be reached by the system as a whole, and where feasible, by different parts of the rail system) • Issuing of **single safety certificates** to railway undertakings → The Agency is the System Authority for the ERTMS
NSAs	• Issuing **safety authorisations** to infrastructure managers • Supervising railway undertakings and infrastructure managers • Issuing, renewing, amending and revoking **certificates granted to entities in charge of maintenance** (or delegate to accredited or recognised bodies) • Monitoring, promoting, and, where appropriate, enforcing and updating the safety regulatory framework including the system of national rule → The Agency and the national safety authorities shall conclude cooperation agreements on issuing single safety certificates to railway undertakings
Railway Undertakings	• Need to hold the **single safety certificate** issued by the Agency or a NSA • Obligation to, where appropriate, **contractually oblige other actors** to implement risk control measures
Infrastructure Managers	• Need to obtain a **safety authorisation** from the national safety authority • Obligation to, where appropriate, **contractually oblige other actors** to implement risk control measures
Accredited /recognised bodies	• Awarding **entity in charge of maintenance certificates** (ECM certificate)
Entities in charge of maintenance	• For locomotives, passenger trains and freight waggons (every vehicle is under the responsibility of one ECM, as registered in the vehicle register): need to hold an **entity in charge of maintenance certificate** (ECM

System Level Actor	Main obligations in context with this deliverable
	certificate) by an accredited or recognised body or by a national safety authority • Obligation to, where appropriate, **contractually oblige other actors** to implement risk control measures

Table 7: Main Obligations of Actors on Interooperability Level

Interoperability Level Actor	Main obligations in context with this deliverable
ERA	• Issuing type / vehicle **authorisations for placing on the market** • Chairing an ERTMS group of notified conformity assessment bodies → The agency is the System Authority for the ERTMS
NSAs	• Authorising the **placing in service** of the trackside control-command and signalling, energy and infrastructure subsystems • Issuing, renewing, amending and revoking vehicle **authorisations for placing on the market,** ensuring that a vehicle number has been assigned
Proposer (actor initialising a significant change to the railway system)	• For **changes to the railway system**: Submitting a **Declaration of risk acceptance** (declaration that all identified hazards and associated risks are controlled to an acceptable level) based on the **safety assessment report**
Assessment Bodies (AsBo)	• Assessing the impact on safety levels and compliance with safety requirements of **changes to the railway system** and provide the proposer with a **safety assessment report** → (AsBo is accredited or recognised for the different areas of competence within the railway system or the NSA itself)
Infrastructure Managers	• Submitting **requests for authorisations of placing in service**, required before any trackside fixed installations can be placed into service (subsystems CCS trackside, energy, Infrastructure) and accompanied by a file which includes: a. **'EC' declarations of verification** of the subsystems b. Technical compatibility of the subsystems with the system into which they are being integrated c. Safe integration of the subsystems d. For subsystems involving ETCS and/or GSM-R equipment:

Interoperability Level Actor	Main obligations in context with this deliverable
	the positive decision of the Agency (ERA) that the technical solutions envisaged are fully interoperable
Railway Undertakings	• Checking that the vehicle has been **authorised for placing on the market** and is **compatible with the route** → May carry out tests in cooperation with the infrastructure manager
Vehicle Keeper	• Registering the vehicle in a vehicle register after the **authorisation to be placed on the market** is granted, and assigning an entity in charge of maintenance
Entities in charge of maintenance	-
Manufacturers	• Submitting **applications for a vehicle / type authorisation for placing on the market**, including: 1. **Placing on the market of the subsystems** forming the vehicle, based on the respective **'EC' declarations of verification** 2. Technical compatibility of the subsystems forming the vehicle 3. Safe integration of the subsystems forming the vehicle 4. Technical compatibility of the vehicle with the network in the area of use • Issuing, in case of vehicle of a particular type authorised for placing on the market: • **Declaration of conformity** to an authorised vehicle type

Table 8: Subsystem Level - CCS Subsystems

Subsystem Level Actor	(as covered by the TSI CCS)
	Main obligations in context with this deliverable
ERA	-
NSAs	-
Railway Undertakings	• Management of errors
Infrastructure Managers	• Management of errors

Subsystem Level Actor	(as covered by the TSI CCS)
Entities in charge of maintenance	-
Manufacturers	• Issuing the **'EC' declaration of verification** (confirming that the subsystem has undergone the relevant verification procedures) • Compiling the **technical file** that is to accompany the 'EC' declaration of verification, containing: o Documents relating to the characteristics of the subsystem o Documents certifying conformity of the interoperability constituents o Elements relating to the conditions and limits of use o Instructions concerning servicing, constant or routine monitoring, adjustment and maintenance Note: In the event of the renewal or upgrading of a subsystem resulting in an amendment to the technical file and affecting the validity of the verification procedures already carried out, the applicant shall assess the need for a new 'EC' declaration of verification. (2016/797 Art 15 clause 5.) • Requesting a NoBo of choice to apply the 'EC' verification procedure (tailored by the presumption of conformity (see: Directive (EU) 2016/797, Article 17) of subsystems which are in conformity with harmonised standards or parts thereof) • Requesting a NoBo of choice to verify the correctness and completeness of the ESC/RSC check report for the subsystem, if applicable • Responsibility of the applicant for subsystem verification: The applicant shall: 1) Ensure that the maintenance requirements as described in [Responsibility of the manufacturer of equipment] are defined for all components within the scope of this TSI regardless of whether or not they are interoperability constituents. 2) Complete the above requirements [...] considering the risks arising from interactions between different components of the subsystem and interfaces to other subsystems. 3) Define procedures for the roll-out of updated interoperability constituents due to specification error corrections (specifications maintenance) according to the relevant documentation of the interoperability constituent, where applicable. The applicant shall provide a configuration management system to identify the impact on the subsystem. The applicant shall ensure the availability of the

Subsystem Level Actor	(as covered by the TSI CCS)
	documentation regarding the version of the interoperability constituents included in its subsystems. - Management of errors
Notified Bodies (NoBo)	- Applying the 'EC' verification procedure using the modules specified in TSI CCS point 6.3.2: for the on-board subsystem either modules SB&SD or SB&SF or SH1; for trackside subsystem either modules SG or SB&SD or SB&SF or SH1 - Issuing the **certificate of verification** - Issuing Intermediate Statements of Verification if requested by the manufacturer - Verifying the correctness and completeness of the ESC/RSC check report for the subsystem, if applicable

Table 9: Subsystem Level – for Interoperability Constituents

Subsystem Level Actor	(for Interoperability Constituents) Main obligations in context with this deliverable
ERA	-
NSAs	-
Railway Undertakings	- Management of errors
Infrastructure Managers	- Management of errors
Entities in charge of maintenance	-
Manufacturers	- Issuing the **'EC' declaration of conformity** (confirming that the interoperability constituents conform to the technical compatibility between ETCS on-board and the trackside parts ETCS of the CCS subsystems within an area of use) - Requesting a NoBo of choice to apply the 'EC' verification procedure (tailored by the presumption of conformity of subsystems which are in conformity with harmonised standards or parts thereof), and choose the modules to be applied for verification (CB&CD or CB&CF or CH1 or CA; see: Directive (EU) 2016/797, Article 17) - Requesting a NoBo of choice to perform ESC/RSC tests, if applicable

Subsystem Level Actor	**(for Interoperability Constituents)** **Main obligations in context with this deliverable**
	• The manufacturer of equipment incorporated in the subsystem shall specify: 1) All maintenance requirements and procedures [...]. For further details on error corrections see points 6.5 (Management of errors) and 7.2.10 (Specifications maintenance (error corrections)) 2) All requirements and procedures (test methods and tools, the required professional competence and the evaluation of the impact of the updated Interoperability Constituent on the subsystem) necessary to implement updated Interoperability Constituents due to specification error corrections throughout the equipment life-cycle (specifications maintenance). This includes the definition of the necessary procedures for updates of approved system modules and processes, during all life cycle phases, when there are error corrections according to Article 9 of this Regulation applicable to the subsystems. 3) [...] 4) The conditions for first line maintenance, i.e. the definition of Line Replaceable Units (LRUs), the definition of approved compatible versions of hardware and software, the procedures for replacing failed LRUs, the conditions for storing LRUs and for repairing failed LRUs. 5) [...] 6) The checks to be carried out when maintaining equipment other than Control-Command and Signalling equipment and which influences the Control-Command and Signalling Subsystems (e.g. changing the wheel diameter). • Management of errors
Notified Bodies (NoBo)	• Issuing the **Certificate of Conformity** • Assessing the conformity based on the chosen modules to be applied for verification (CB&CD or CB&CF or CH1 or CA) and based on table 6.1.1. and, in case of on-board ETCS, the mandatory test set out in 6.2.4.1. • Performing ESC/RSC tests

APPENDIX C

During Task 3, several workgroups have analysed different integration and maintenance roles and activities in the context of the MPC and the Modular Platforms Architecture of D26.3 [5] and the scenarios provided by the System Pillar CE document “Operational Analysis Specification” [10].

The following five areas have been identified and analysed:

Integration & maintenace-1	Functional Systems (FS) with CEME-Virtualisation Environments (VE)
Integration & maintenace-2	Functional Systems with CEME-NHA
Integration & maintenace-3	Functional Systems with Platform Management
Integration & maintenace-4	Platform Management with Virtualisation Environment
Integration & maintenace-5	Platform Management with Shared Services

As part of the analysis and discussions between the WP26 partners from railways and industry, several tables have been derived, identifying the involved acting roles “Accountable, Responsible, Consulting”, their potentially to be performed Activities, received Input and generated Output

Not all existing tables have been integrated into this Appendix on purpose since all performed analysis follow the same pattern and additional tables won’t provide added value to the reader.

We present here the results on the first activities along “Functional Systems (FS) with CEME-Virtualisation Environments (VE)”, providing two integration and two maintenance scenarios:

- Table 10: Functional System integrated with Virtualisation Environment in context of the safety case
- Table 11: Functional System integrated with Virtualisation Environment in context of the initial deployment in a given data centre
- Table 12: Functional System integrated with Virtualisation Environment after update of the VE, not affecting the interface to the FS
- Table 13: Functional System integrated with Virtualisation Environment after update of the VE, affecting the interface to the FS

Table 10: Functional System integrated with Virtualisation Environment in context of the safety case

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
01a	VE	Order VE (Make, Model, Version)	harmonised or FS supplier specific requirements to VE	FS Supplier	FS Supplier		confirmed commercial order
01b	VE	Supply VE	confirmed commercial order	VE Supplier	VE Supplier		VE with full version identification and user & maintenance documentation available at FS supplier premises
02a	VE	install VE in FS supplier test lab	VE + documentation + installation support	FS Supplier	FS Supplier	VE Supplier	VE installed in FS supplier test lab
02b	VE	qualify VE against VE requirements (prior to integration)	VE + requirements to VE + qualification test set	FS Supplier	FS Supplier	VE Supplier	VE qualified

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
03	FS + VE	integrate FS with VE	FS + VE + integration test set	FS Supplier	FS Supplier	VE Supplier	FS + VE integrated (+ possibly findings-change requests against FS-retest until integration successful) OR new VE qualification requirements + test set
04a	FS + VE	validate FS running on VE	FS + VE + entire FS test sets	FS Supplier	FS Supplier		FS validated running on VE (+ possibly findings-change requests against FS-retest until validation successful without findings/open points concerning FS-VE integration) OR new VE qualification requirements + test set

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
04b	VE	only if necessary (to avoid if possible): integrate new requirements and test sets FS to VE into harmonised requirements and test sets for VE qualification	new requirements and test sets to VE	owner of VE qualification requirements and test sets	FS Supplier	VE supplier, harmonisation stakeholders	new harmonised VE qualification requirements and test sets
05	FS	have FS ('generic application') assessed, certified and authorised (as far as applicable for generic application)	FS + FS documentation incl. requirements to VE operation & maintenance + requirements to VE + according test sets	FS Supplier	FS Supplier		FS deployable on VE

Table 11: Functional System integrated with Virtualisation Environment in context of the initial deployment in a given data centre

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
00	FS + VE	establish safety organisation for the operation and maintenance of the FS on the VE	contracts between FS Supplier, FS Operator and PF Owner; operation & maintenance documentation of the FS; regulatory provisions on operation and maintenance of the FS and of the platform (e.g. data centre)	FS Operator	FS Operator, FS Supplier, PF Owner		valid organisation and contracts matching the operation & maintenance documentation of the FS and the regulatory provisions on operation and maintenance of the FS and of the platform (e.g. data centre)

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
01	VE	provide FS Supplier with information on target VE to run the FS	contracts between FS Supplier, FS Operator and PF Owner; operation & maintenance documentation of the FS; regulatory provisions on operation and maintenance of the FS and of the platform (e.g. data centre)	PF Owner	PF Owner		identification and existing qualification documentation of target VE
02a	FS + VE	verify that FS requirements for VE match existing VE qualification	VE + requirements to VE + existing VE qualification	FS Supplier	FS Supplier	PF Owner	VE qualified for FS OR: no match, then VE needs to be qualified against FS (see step 02b)
02b	FS + VE	if necessary: qualify VE against VE requirements (prior to integration)	VE + requirements to VE + qualification test set	FS Supplier	PF Owner	VE Supplier	VE qualified for FS

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
03	FS	provide FS to PF Owner	FS + documentation	FS Supplier	FS Supplier		FS + VE ready for integration on PF Owner premises
03a	FS + VE	deploy FS on VE	FS + integration test set	PF Owner	PF Owner	FS Operator	FS + VE integrated OR: additionally, some test findings necessitating step 03b
03b	FS + VE	if necessary: perform any FS modification necessary and then re-deploy (03a)	integration test set findings + FS	FS Supplier	FS Supplier		modified FS as input for step 03a
04a	FS + VE	validate FS running on VE	FS + VE + final FS validation test sets	FS Supplier	FS Supplier	FS Operator	FS validated running on VE (+ possibly findings-change requests against FS-retest until validation successful without findings/open points concerning FS-VE integration)

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
04b	FS	if necessary worst case scenario: default back to scenario FSVE_PIO_Scenario1	test findings that do not allow for safe integration of given FS + VE versions	FS Supplier	FS Supplier		possibly: new harmonised VE qualification requirements and test sets exit to scenario: FSVE_PIO_Scenario1 re-entry here at step 03 with FS deployable on VE
05a	FS	have FS instantiation ('specific application') assessed and certified* *: certifications in FS Supplier responsibility	FS + FS documentation incl. validation report and incl. requirements to VE operation & maintenance + requirements to VE + according to test sets	FS Supplier	FS Supplier		FS supplier obligations to establish operation of FS on VE are fulfilled

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
05b	FS	have FS instantiation ('specific application'), certified* and authorised: certifications in FS Operator responsibility	FS + FS documentation incl. validation report and incl. requirements to VE operation & maintenance + requirements to VE + according to test sets	FS Operator	FS Operator		FS authorised for operation on VE

Table 12: Functional System integrated with Virtualisation Environment after update of the VE, not affecting the interface to the FS

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
01	VE	build and test new VE version	contracts between FS Supplier, FS Operator and PF Owner; operation & maintenance documentation of the FS; regulatory provisions on operation and maintenance of the FS and of the platform (e.g. data centre)	PF Owner	VE supplier		target VE version with release notes
02a	VE	qualify VE against orchestration SW requirements	VE + requirements to VE + qualification test set (orchestration SW)	PF Owner	PF Owner		VE qualified for orchestration SW (OR: back to step 01)
02b	FS + VE	qualify VE against VE requirements (prior to integration)	VE + requirements to VE + qualification test set (FS)	FS Supplier	PF Owner	VE Supplier	VE qualified for FS (OR: back to step 01)

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
02c	FS + VE	agree on roll out plan	contracts + release notes + qualification test set results	FS Supplier	PF Owner	FS Operator	agreed roll out plan
03a	FS + VE	deploy FS on VE (first integration)	FS + integration test set	PF Owner	PF Owner	FS Operator	FS + VE integrated OR: additionally, some test findings necessitating step 03b
03b	FS + VE	if necessary worst case scenario: default back to scenario FSVE_Maintenance_Scenario2a	integration test set findings + FS	FS Supplier	FS Supplier		modified FS as input for step 03a
04	FS + VE	update documentation related to certification and approval of FS and put FS on new VE version into commercial service	FS + VE + their documentation+ integration test reports	FS Supplier	PF Owner	FS Operator	FS running on new VE version in commercial service, documentation and configuration management up to date

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
05a	FS	FS performance is observed for a period of time (length of period depends on how urgent the VE update is considered, for instance in the case of security issues), w.r.t. whether the FS replica on old and new VE deliver the exactly same results	FS + VE	FS Supplier	PF Owner		FS supplier obligations to establish operation of FS on VE are fulfilled
05b	FS + VE	deploy all further instances according to deployment plan	FS + VE	PF Owner + FS Supplier	PF Owner	FS Operator	new VE version is rolled out

Table 13: Functional System integrated with Virtualisation Environment after update of the VE, affecting the interface to the FS

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
01	VE	build and test new VE version	contracts between FS Supplier, FS Operator and PF Owner; operation & maintenance documentation of the FS; regulatory provisions on operation and maintenance of the FS and of the platform (e.g. data centre)	PF Owner	VE supplier		target VE version with release notes
02a	VE	qualify VE against orchestration SW requirements	VE + requirements to VE + qualification test set (orchestration SW)	PF Owner	PF Owner		VE qualified for orchestration SW; handed over to FS supplier (OR: back to step 01)
02b	FS + VE	qualify VE against VE requirements (prior to integration)	VE + requirements to VE + qualification test set (FS)	owner of VE qualification requirements and test sets	PF Owner	PF Owner, VE Supplier	VE qualified for FS (OR: back to step 01 OR: FS needs update, go to FSVE_Maintenance_Scenario 2b)

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
02c	FS + VE	agree on roll out plan	contracts + release notes + qualification test set results	FS Supplier	PF Owner		agreed roll out plan
03a	FS + VE	deploy FS on VE (first integration)	FS + integration test set	PF Owner	PF Owner	FS Operator	FS + VE integrated OR: additionally, some test findings necessitating step 03b
03b	FS + VE	if necessary worst case scenario: default back to scenario FSVE_Maintenance_Scenario2a	integration test set findings + FS	FS Supplier	FS Supplier		modified FS as input for step 03a
04	FS + VE	validate FS running on VE and update documentation related to certification and approval	FS + VE + final FS validation test sets	FS Supplier	PF Owner	FS Operator	FS validated running on VE (validation requiring presumably only minimal effort, like checking right versions), FS running on new VE version in commercial service, documentation and configuration management up to date

ID	Related components	Activities	Input	Accountable	Responsible	Consulting	Output (Artefacts + Tools etc.)
05a	FS	FS performance is observed for a period of time (length of period depends on how urgent the VE update is considered, for instance in the case of security issues), w.r.t. whether the FS replica on old and new VE deliver the exactly same results	FS + VE	FS Supplier	PF Owner		FS supplier obligations to establish operation of FS on VE are fulfilled
05b	FS + VE	deploy all further instances according to deployment plan	FS + VE	PF Owner	PF Owner	FS Operator	new VE version is rolled out