



ERJU SYSTEM PILLAR

# **TCCS\_E2E Data Process for the Digital Railway- Cover Document**




System pillar – CONEMP

# **End-to-end data process for the Digital Railway System - paving the way towards CONEMP, the life-**

# cycle asset management



Author(s)	Ralph R Müller , Boryana Tezgetarska , Benedikt Wenzel , Karl-Albrecht Klinge
Abstract	This document aims to describe the E2E Data Process of the CONEMP Domain, from planning to commissioning of safety-critical and operational data. It covers four phases: generic data preparation, supplier configuration, integration, and system distribution. The process ensures a continuous, secure, and interoperable data flow across the digital railway infrastructure.
Config Item	Document and Release Plan
Document ID	TCCS Sector Review Process 2025/TCCS_E2E Data Process for the Digital Railway- Cover Document#726315  TCCS_E2E Data Process for the Digital Railway- Cover Document
Classification	Public
Status	Released
Version	1.0
Revision	726315
Last Change Date	06.10.2025
Copyright	Brussels: Europe's Rail Joint Undertaking, 2025

© Europe's Rail Joint Undertaking, 2025

This document is drafted by and belongs to EU Rail.

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

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

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

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

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

## Document History

1.0 06.10.2025	Boryana Tezgetarska	Approved version based on Review X.X
----------------	---------------------	--------------------------------------

## Review description

Type of Approval	 Document Review
------------------	---

## Approval description

Type of Approval	 Document Approval
------------------	---

## Contents

1	Introduction	7
2	System Pillar for digital rail implementation	13
2.1	System pillar standardisation scope	13
2.2	Interfaces and data transfer	14
3	CONEMP rules the assets lifecycle	14
3.1	CONEMP for the railway system	14
4	Core of CONEMP: E2E data process	15
4.1	Overview of the E2E Process Phases	15
4.2	High-level data flow for Configuration	15
4.3	Phase 1 – Generic safety-relevant data prep	17
4.3.1	How to get configuration data? Prepare it!	17
4.4	Supplier data configuration	19
4.5	Configuration data integration	20
4.6	Configuration data distribution (SFC)	21
4.6.1	Problem Statement	22
4.6.2	Configuration Interfaces and Standards	22
4.6.3	Solution Approach	23
4.6.3.1	Service Function Configuration	23
4.6.3.2	The Role of SMI v3	23
4.6.3.3	Dependency Management Across Field Elements and Control Systems	24
4.6.3.4	Metadata Structures for Distribution and Orchestration	24
4.6.3.5	Safety Attestation and Separation of Responsibilities	24
4.6.4	Configuration Process Overview	24
4.6.5	Summary	26
4.7	Demonstration E2E Process	27
5	Safety	30
6	Security	30
7	Is the system running well and how will it do? Diagnostics will tell- if it can!	30
7.1	Diagnostics Limitations	30
7.1.1	Operational Limitations	30
7.1.2	Tactical Limitations	31
7.1.3	Strategic Limitations	31
7.1.4	Need for Standardised Diagnostics	31
7.2	Diagnostics Interfaces and Standards	31

7.3 Service Function Diagnostics	32
7.3.1 Generic and Product-Specific Models	32
7.3.2 Semantic Representation and Toolchain Support	32
7.3.3 ERP and System Integration	32
7.3.4 Diagnostics Harmonisation and Sector Impact	32
7.4 Summary	33
8 OPC-UA for communicating Diagnostic Data	35
8.1 Structured Information Models	35
8.2 Hierarchical and Functional References	35
8.3 Semantic Integration and Historical Access	35
8.4 Historical Data and Event Integration	35
8.5 Built-In Features for Secure and Scalable Operation	36
8.6 Communication Protocol and SDK Support	36
9 Catalogue of Symbols: The Europeaniser for railway staff	36
10 Reference Implementation	38
11 More to come: SERA takes it all!	38
12 References	39
13 Annex: Delivery Process	40

Figure 1. 0 The Service Function Configuration architectural components

## 1 Introduction

The EU-RAIL System Pillar CONEMP domain provides systems, SIL 4 platform architecture, standard protocols, and data structures for functionalities that are needed on network level and for engineering use cases<sup>(Remit given by ERJU Service Contract 2.4)</sup>.

Therefore, EU-RAIL System Pillar CONEMP Domain is delivering the following contributions to SERA:

- **Extension of the ERA-ontology** based on evolving CCS/TMS use cases.
- **The “Catalogue of Symbols”** as the addendum to the ERA-ontology where user interfaces are addressed, and a standardised representation and control of information is beneficial.
- **Data preparation:** Enabling project-specific data engineering for SERA (ETCS-only) and validating against ERA-ontology and further formalised engineering rules with the help of the “Interoperability Test Bed” (ITB). Config templates, e.g. for ETCS-trackside, support the provider of data.
- **Service Function Configuration:** based on prior prepared and validated data, handover to product suppliers, receiving suppliers' config data stored in config repositories for uptake and processing. In a decentralised modular railway system, data from various config repositories needs to be provided to data-consuming systems in an orchestrated, safe, and secure process: the Service Function Configuration.
- **Service Function Diagnostics:** providing controlled and managed shared data (e.g. by Data Spaces, integration layers, ...), based on the generic equipment model (SDI-GEN) that ensures interoperability of the data points defined by product group models specific to each technical product.
- **Risk Analysis:** A comprehensive risk analysis supports the decisions taken for the Service Function Configuration
- **Compute Environment (CE):** Provides the specification of Computing Environment interfaces I2 (Hardware Abstraction interface) and I3 (Virtualisation interface) to host SIL-4 Functional System. Furthermore, the specification of I1 interface (maintenance, diagnostic and security). The upcoming integration of CE specifications into CONEMP has been prepared by the applicability of the Service Functions Configuration and Diagnostics to the specific constraints of a CE. CONEMP is agnostic to architecture.

After railway sector approval and publication of the ERA-ontology including CCS/TMS and the Configuration and Diagnostics concept in 10/2024, the full integration into ERA-ontology and the specification of the service functions configuration and diagnosis down to the bottom (architecture level 5 – product architecture) has been accomplished and is awaiting rail sector approval for EU-RAIL internal publication by 10/2025 (see Release note ISPR0.0, especially sections 1.2 and 1.3).

The current E2E Data Process will be embedded into the wider context of CONEMP, the lifecycle process for asset management, from end of 2025 on. It is recognised that CONEMP deliverables shall be taken up by the next wave of Innovation Pillar projects from 2026 on to allow testing of and feedback to the specification. Also, all other domains of the System Pillar need to integrate and commit to the CONEMP deliverables for full system integration success and operational maturity proof. CONEMP must be derived from a holistic, cross-domain concept along a top-down process, which ensures consistency from the beginning. Therefore, the unrestricted publication of the service functions is foreseen by the end of the System Pillar in 2027. The aim of this document is to inform high-level about the state of the current work and its implications (sections 3-8) in order to allow the sector to early prepare for the sector alignment process of the EU-RAIL internal publication as described below.

### TCCS Document Tree

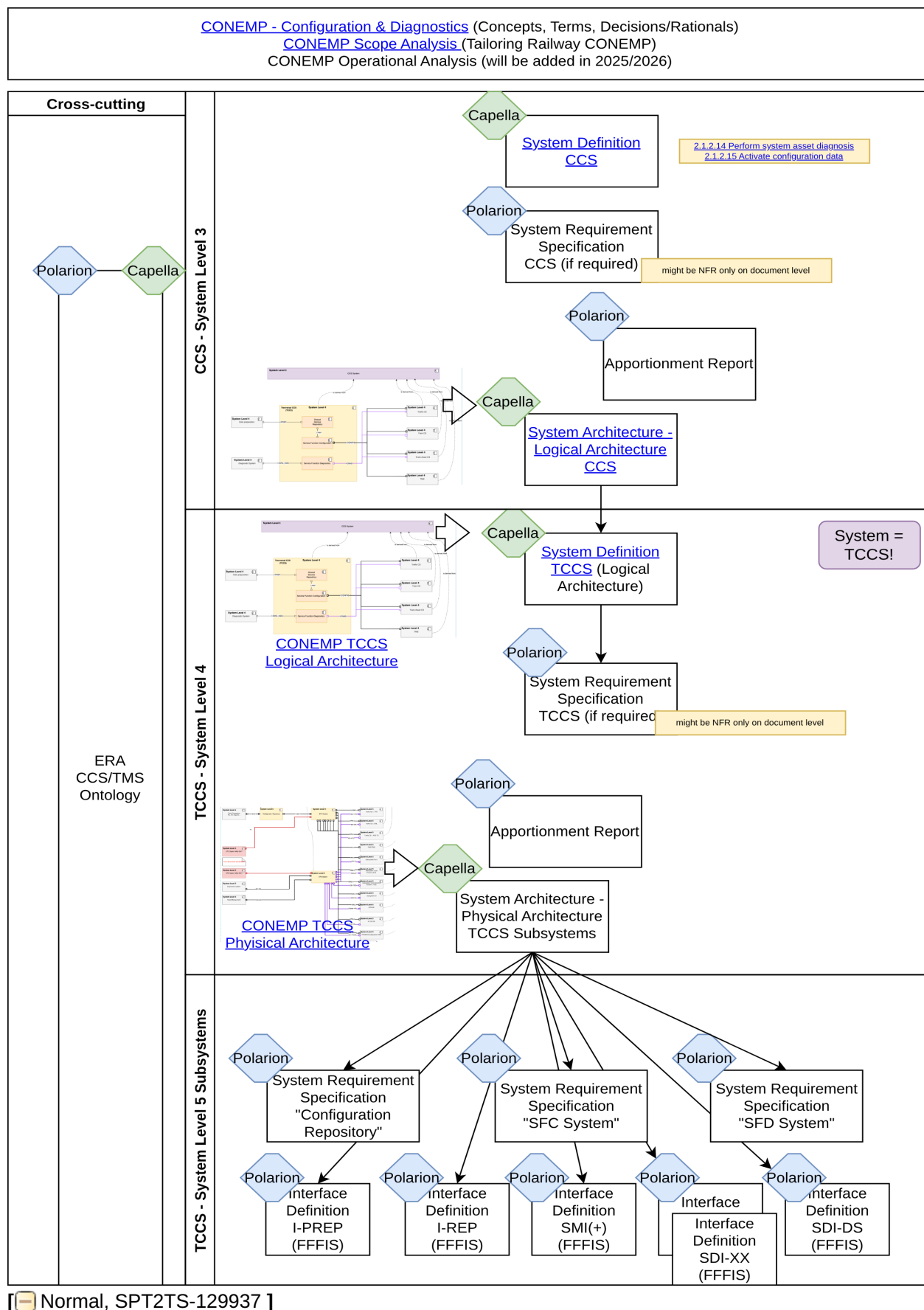








Figure 1 Document Tree




## TCCS Deliverables SC2.4

The following deliverables are provided by the TCCS/CONEMP domain for the transversal CCS functionality of configuration & diagnostics incl. ERA Ontology integrated data structure for configuration, diagnostics and communication:

System Level	Interface or System Name	Document Title/ Name	Model Generated	Polarion Link	State	Approval by (priority recommendation)
SL3-5	CCS/TMS systems and interfaces	ERA CCS TMS ontology (CCS/TMS Data Model for Configuration and Communication)	no	TCCS - CCS/ TMS Data Model enabled by ERA Ontology - Cover Document	Ready for SP review	All domains (Focus on ERA CCS TMS ontology (data model) content used at interfaces and for configuration of your domain)
SL4	Transversal CCS	TCCS Risk Analysis	partially	Transversal CCS- System definition - SL4 - Risk Analysis	Ready for SP review	All domains
SL4 (LA)	TCCS system	TCCS System Definition	partially	 TCCS System Definition	Ready for SP review	All domains
SL4 --> SL5 (PA)	TCCS system	TCCS System Architecture - TCCS subsystems	partially	 TCCS System Level 5 - System Architecture Description	in progress	All domains
SL5 (PA)	Service Function Diagnostics and Diagnosable BuildingBlock (SERA Version)	TCCS SRS Service Function Diagnostics and Diagnosable BuildingBlock	partially	<i>SPT2TS/TCCS Service Function Diagnostics _SFD_ L5/ TCCS SRS Service Function</i>	Ready for SP review	All domains (i.e. TCCS/CONEMP for this internal TCCS/ CONEMP subsystem/ interface)

System Level	Interface or System Name	Document Title/ Name	Model Generated	Polarion Link	State	Approval by (priority recommendation)
				<i>Diagnostics and Diagnosable BuildingBlock : 726315</i>		
SL5 (PA)	SDI-XX (SERA Version)	TCCS System Interface SDI-XX Base	partially	<i>SPT2TS/TCCS Service Function Diagnostics _SFD_ L5/ TCCS System Interface SDI-XX Base : 726315</i>	Ready for SP review	All domains
SL5 (PA)	SDI-DS (SERA Version)	TCCS System Interface SDI-DS information model	yes	<i>SPT2TS/TCCS Service Function Diagnostics _SFD_ L5/ TCCS System Interface SDI-DS information model : 726315</i>	Ready for SP review	All domains (i.e. TCCS/CONEMP for this internal TCCS/CONEMP subsystem/interface)
SL5 (PA)	SDI-GEN (SERA Version)	TCCS System Interface SDI-GEN information model	yes	<i>SPT2TS/TCCS Service Function Diagnostics _SFD_ L5/ TCCS System Interface SDI-GEN information model : 726315</i>	Ready for SP review	All domains
SL5 (PA)	Reference application of SFD toolchain with the example	TCCS System Interface SDI-P information model	yes	<i>SPT2TS/TCCS Service Function Diagnostics</i>	Ready for SP	All domains (i.e. TCCS/CONEMP, TACS, Traffic CS)

System Level	Interface or System Name	Document Title/ Name	Model Generated	Polarion Link	State	Approval by (priority recommendation)
	SDI-P (SERA Version)			<i>_SFD_ L5/ TCCS System Interface SDI-P information model : 726315</i>	review	
SL5 (PA)	SMI (v3) (SERA Version)	TCCS System Interface (impl. I_CONFIG) <ul style="list-style-type: none"> <li>• TCCS System Interface SMI (v2) to SMI (v3)</li> </ul>	partially	<i>SPT2TS/TCCS Service Function Configuration _SFC_ L5/ TCCS System Interface SMI_v3_ _impl_ I_CONFIG_ : 726315</i> <ul style="list-style-type: none"> <li>•  System Requirements Specification_TCCS-System Interface SMI (v2) to SMI (v3) Change Requests</li> </ul>	Ready for SP review	All domains
SL5 (PA)	Configuration Repository (SERA Version)	TCCS SRS Configuration Repository incl. Data Prep (Content and Rules for E2E Phase 1 - Generic safety relevant data prep)	partially	 System Requirements Specification_TCCS - Part 2 Configuration Repository (SERA Version)	Ready for SP review	All domains (i.e. TCCS/CONEMP for this internal TCCS/CONEMP subsystem/interface)

System Level	Interface or System Name	Document Title/ Name	Model Generated	Polarion Link	State	Approval by (priority recommendation)
SL5 (PA)	Service Function Configuration and Configurable BuildingBlock (SERA Version)  <i>incl Risk Analysis SL5 SFC</i>	TCCS SRS Service Function Configuration and Configurable BuildingBlock	partially	 System Requirements Specification_TCCS - Part 3 Service Function Configuration and Configurable BuildingBlock (SERA Version)  <i>incl Risk Analysis SFC</i>	Ready for SP review	All domains (i.e. TCCS/CONEMP for this internal TCCS/CONEMP subsystem/interface)
SL5 (PA)	I-REPO (SERA Version) ( <i>I-REP, I-PREP</i> )	TCCS System Interface REPO	partially	 System Interface Description_TCCS-System Interface REPO (SERA Version) (part of I-PREP might be extracted to an additional document)	Ready for SP review	All domains (i.e. TCCS/CONEMP for this internal TCCS/CONEMP subsystem/interface)
SL5 (PA)	Catalogue of Symbols (CoS)  <i>ERA-ontology extension for UI</i>	Catalogue of Symbols (CoS)	partially	 System Concept_TCCS-Catalogue of Symbols	Ready for SP review	All domains
SA (PA)	List of SRACs  <i>exported constraints</i>	List of safety-related application conditions (SRAC)	no	pending	starting 10/2025	All domains

System Level	Interface or System Name	Document Title/ Name	Model Generated	Polarion Link	State	Approval by (priority recommendation)
	to other domains					

[=] Normal, SPT2TS-130464 ]


Table 2 SC2.4. CONEMP TCCS (Transversal CCS) deliverables

## 2 System Pillar for digital rail implementation

EU's System Pillar is the sector forum to harmonise interfaces and does further steps for standardising the entire CCS and its associated processes in line with the overall policy of ERA towards digital interfaces (see figure below). In addition to TMS/CMS and trains, there are detailed specifications for the three exchangeable systems ATO-TS, PES and ETPS. The harmonised system specifications contain all external interfaces, functional and non-functional requirements and a precise behaviour description (linking inputs and outputs depending on the system state). The harmonised specifications are written solution-neutral, allowing various forms of product implementation.. This applies as well for the specifications delivered by CONEMP which can be applied to all non-mandatory implementation forms (e.g. RBC/IXL) in line with the ETPS specifications. The target is to have final specifications which will be complete, precise, unambiguous, verifiable, testable, and maintainable. In other words, the 4 C shall apply:

- complete
- correct
- concise
- confirmable.

42



# Digital Interfaces

- The railways, albeit with some delays compared to other industries, are moving towards interfaces and information flows based on a digital approach.
- Digital interfaces enable error control, modularisation, scalability, vendor independence. Adopting an IP-based, layered approach enables decoupling the information/control flow from the communication technology.
- Moving away from vendor specific, dedicated, analog wirings to (open) networks based on standard protocols brings significant benefits.
- However, there is also a need to master the field of cybersecurity.

Figure 2 Benefits and risks with digital interfaces (Extract from ERA presentation "EU Railway System Architecture - ERA Requirements" dated 17th of January 2024)

### 2.1 System pillar standardisation scope

Scope of standardisation within the system pillar for TCCS and next steps for refinement and alignment:

- Contribution to ERA ontology
- Catalogue of Symbols as the UI namespace of ERA ontology
- Generic safety-relevant data prep process standardisation, including data validation and config templates
- Configuration process standardisation

- Infrastructure configuration data, Vehicle configuration data
- Definition of dependency tree for the Infrastructure Configuration Data
- SMI v3 interface for the distribution on board and trackside
- SDI interface for the collection of diagnostic data
- Service function configuration and service function diagnostic systems
- Interfaces I-REP to enable downloading the configurations available from Configuration Repositories
- CE standardisation scope

[ Normal, SPT2TS-131070 ]

## 2.2 Interfaces and data transfer

To support the digital transformation of railway systems, a unified approach is needed that consolidates configuration and safety attestation into a single, automated interface. It must allow explicit dependency management, version control, and secure update workflows. It must establish a harmonised diagnostics framework that enables cross-supplier interoperability and scales across both trackside and onboard systems, supporting thousands of heterogeneous devices.

Without this integration, railway operations will remain dependent on manual interventions, non scalable tooling, and fragmented safety assurance processes—undermining efficiency, reliability, and long-term maintainability.

**SMI:** Configuration data is considered “static data”: Any change to static data results in a new version of the system. Safety related and non-safety related configuration data is communicated via SMI.

**SCI:** Via SCI safe dynamic data is exchanged between two communicating sub-systems. Change of dynamic data does not result in a new version of the system.

**SDI:** Diagnostic data is communicated via SDI (Standard Diagnostic Interface). SDI data is by definition non-safe data. SDI is not only used to communicate diagnostic information but also non-safety related temporary states like braking performance or traction limitations.

**SSI:** Security services like, IAM (identity and access management), time Synchronisation, certificate management...etc, are provided through the SSI interfaces to all CCS subsystems.

**OPC UA** (Open Platform Communications Unified Architecture) is chosen as the core technology for both the modeling and communication aspects of the Service Function Diagnostics and Configuration frameworks due to its unique combination of flexibility, extensibility, and built-in security features. Unlike traditional protocols, OPC UA is not just a communication protocol - it is a semantic modeling framework that enables structured, interoperable information exchange across complex and heterogeneous systems.

## 3 CONEMP rules the assets lifecycle

### 3.1 CONEMP for the railway system

CONEMP = Concept Of Employment, which refers to a strategic framework that outlines how forces are employed to accomplish a mission or objective within a specific operational context. There are generic standards like ISO/IEC 15288: 2023 that define CONEMP on a general level. We deliver the railway-specific interpretation based on industrial standards, i.e. the "Railway-CONEMP". Railway-CONEMP is fully compliant with the industrial CONEMP applied to the SERA digital railway system.

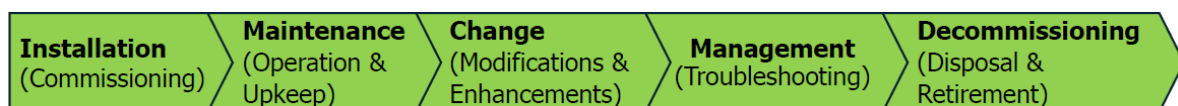



Figure 3 EU CONEMP process (lifecycle)

A detailed analysis regarding the relevance of CONEMP activities for railways and evaluating how it matches with the scope of the System Pillar is done in the  CONEMP - Scope Analysis. (<https://>

polarion.rail-research.europa.eu/polarion/#!/project/SPT2TS/wiki/30%20TCCS%20Deliverables/CONEMP%20-%20Scope%20Analysis ) [📄 Normal, SPT2TS-131200 ]

## 4 Core of CONEMP: E2E data process

### 4.1 Overview of the E2E Process Phases

Overview of end-to-end process, from data preparation to system configuration

As represented in the figure below, the process starts with the generic **safety-relevant data preparation phase** (E2E phase 1) based on ERA CCS TMS ontology.

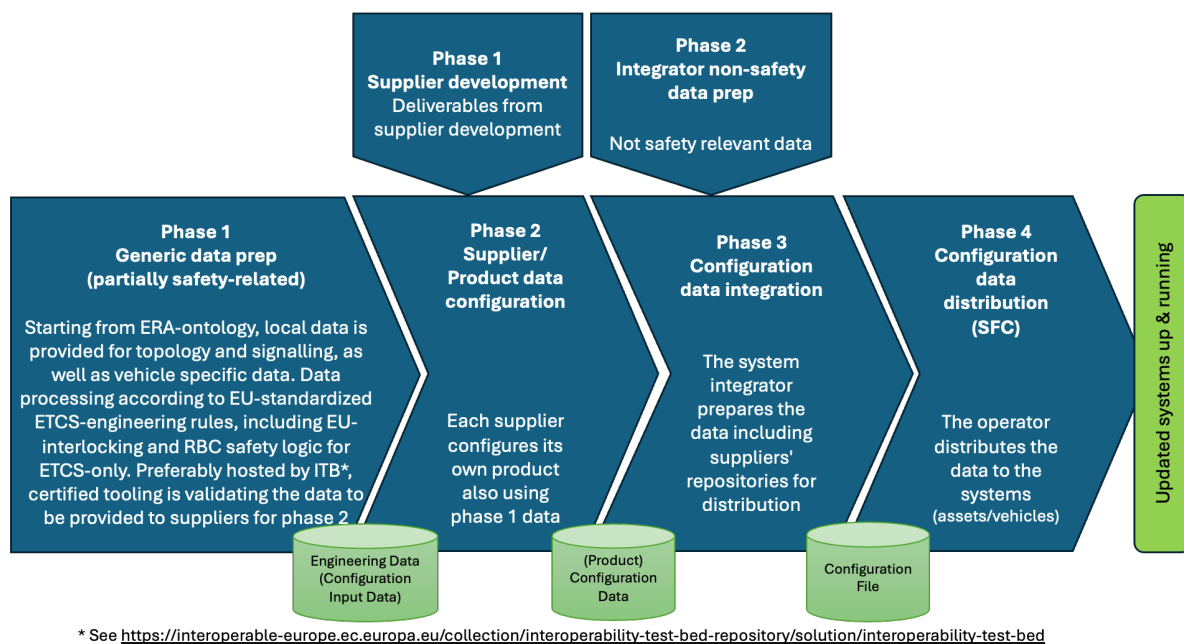


Figure 4 Overview E2E Process

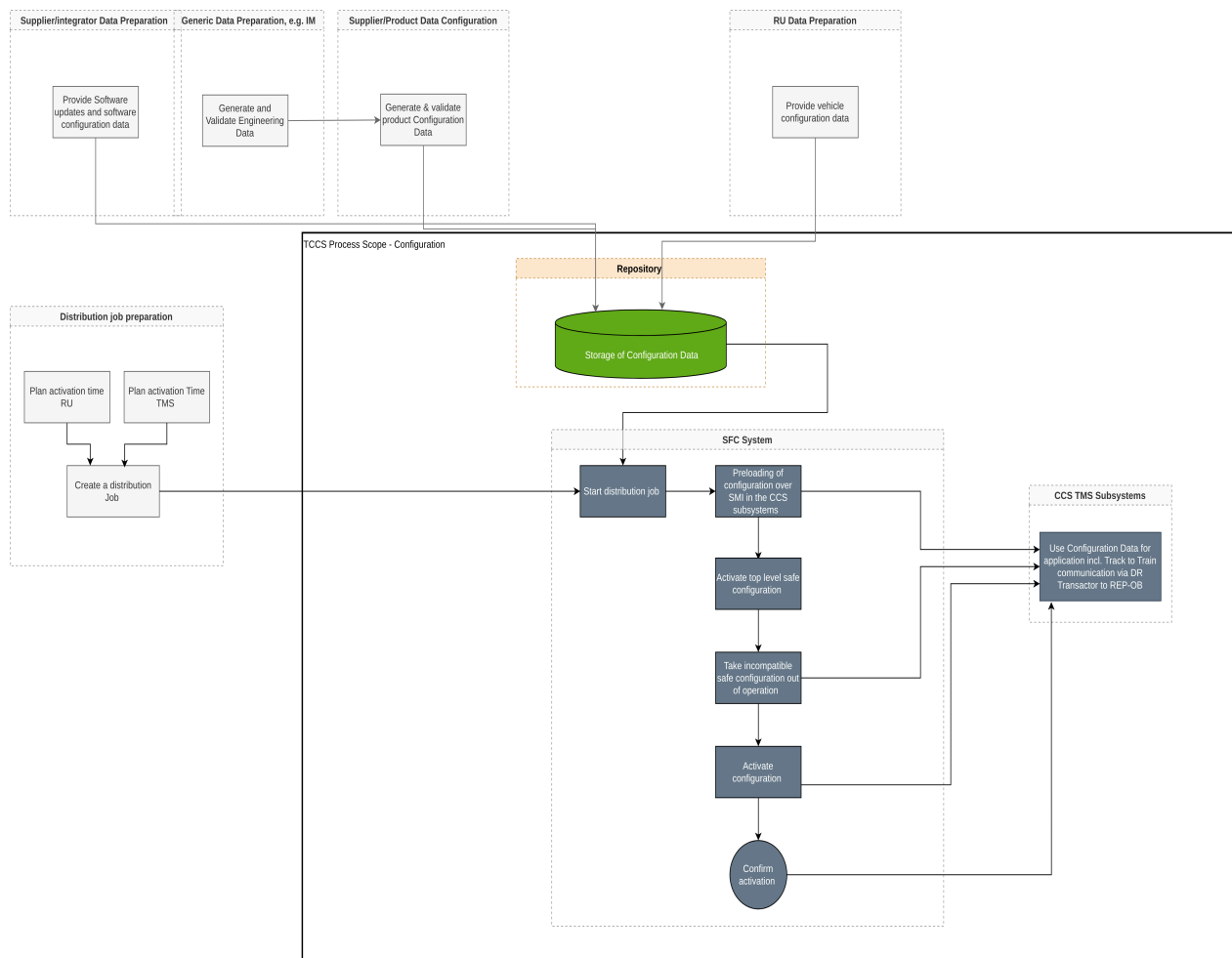
The engineered and validated 📄 SPT2TS-127778 - Engineering data (see [Interoperability Test Bed - ITB](#) ) is handed over to suppliers, enabling them to perform the **supplier data configuration** (E2E phase 2). The compiled data resulting from the supplier data configuration phase is processed by the system integrator in the **configuration data integration** (phase 3), stored in corresponding repositories represented in the subsystem 📄 SPT2TS-127814 - Configuration Repository and made available for the **configuration data distribution** (phase 4), see 📄 SPT2TS-49108 - Configuration Management Process, to distribute and activate the data in the CCS Systems and TMS. [📄 Normal, SPT2TS-131194 ]




The installed assets in the field represent the "single source of truth" for the asset management. This is ensured by Service Function Diagnostics, which furthermore monitors the technical status and health of the systems for timely intervention before the availability of components may deteriorate. [📄 Normal, SPT2TS-131196 ]

### 4.2 High-level data flow for Configuration


#### High-level data flow - from data preparation to system configuration



The illustration below provides an overview of the high-level data flow involving the different SL5 systems (identified in 📄 SPT2TS-127880 - TCCS Architecture) of the Transversal CCS for Configuration.





As pointed out in the phases of the  SPT2TS-131194 - Overview of end-to-end process, from data preparation to system configuration, the configuration starts with the data preparation phase, including product-specific amendments and final compilation of Configuration Data. The compiled data resulting from the data preparation phase is stored in corresponding repositories represented in the subsystem  SPT2TS-127814 - Configuration Repository and made available for the  SPT2TS-49108 -

Configuration Management Process to distribute and activate the data in the CCS Systems and TMS.

Based on planned activation times from TMS or RU inputs, the user (operator level) generates a distribution job. The distribution job contains all the needed attributes according to  Logical Concept, including “When” and “What” to update and the dependency tree.

*Note: According to the  Logical Concept, the configuration metadata with the dependency tree will contain the configuration payload. In the case of the infrastructure-related configuration data, the payload would be standardised according to the ERA CCS TMS ontology  CCS/TMS Data Model . The data preparation (phase 1) follows a standardised process. For the configuration data integration (phase 3) of software configuration data, the payload could remain proprietary and is carried by suppliers and integrator.*

A user (operator level) starts the distribution job on the level of  SPT2TS-128018 - Service Function Configuration System, leading to the preloading of configuration over configuration interface in CCS subsystems and potentially TMS.

The top-level safe configuration activation is then started after receiving the command from the user (operator level), which starts the phase of deactivation of incompatible Building Block configurations and incompatible safe configuration is taken out of operation: this step is planned to be done through the safe configuration authority (SCA) of the  SPT2TS-128018 - Service Function Configuration System, which still needs refinement regarding the orchestrating mechanism in details in the next steps.

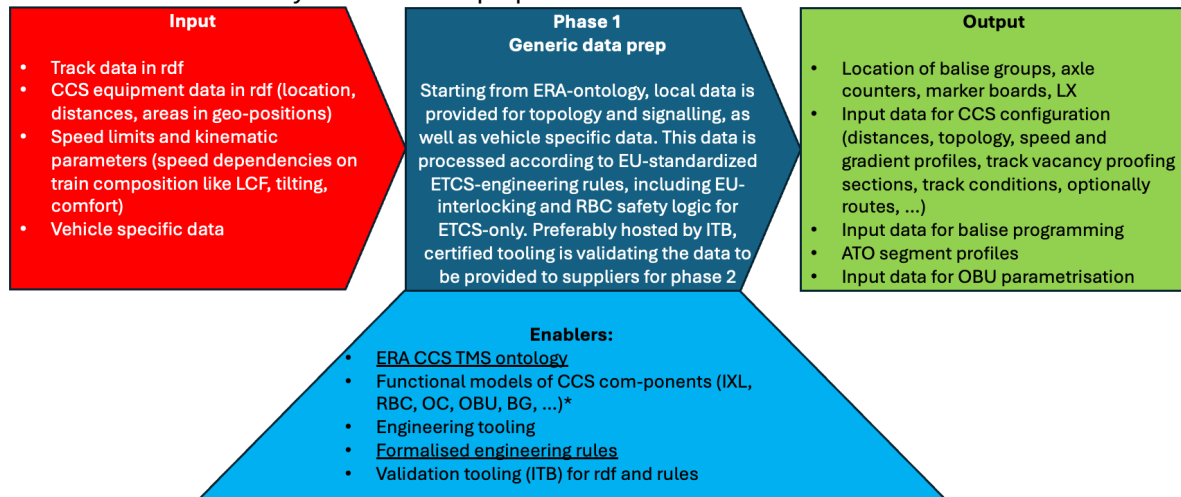
Finally, the activation is started, and a confirmation is needed to ensure the successful activation of the updated configuration.

 Normal, SPT2TS-129025 ]



### 4.3 Phase 1 – Generic safety-relevant data prep

#### Phase 1 – Generic safety-relevant data prep



\* Also known as “Generic Application”

Figure 5 Generic safety-relevant data prep


#### Links:

- ERA CCS TMS Ontology: [https://gitlab.com/era-europa-eu/public/interoperable-data-programme/era-ontology/era-ontology/-/tree/ext-ccstms?ref\\_type=heads](https://gitlab.com/era-europa-eu/public/interoperable-data-programme/era-ontology/era-ontology/-/tree/ext-ccstms?ref_type=heads)
- Formalised Engineering Rules: *SPT2TS/System Level 4/Data preparation rules : 726315* (live document)

[📄 Normal, SPT2TS-130951 ]

#### 4.3.1 How to get configuration data? Prepare it!

For a connected digital system, data must be structured using a “common language”, widely known as data model. The SERA data models are all derived from ERA ontology. The purpose of the ERA CCS TMS ontology is two-fold:

- It has to ensure the enabling, generation, validation and provision of  SPT2TS-127778 - Engineering data to the product configuration, which produces configuration data with standardised and product-specific payload.
- And it has to ensure the consistency of data at SCIs. Data exchanged via SCIs are data generated by the communicating systems and, if needed, data derived from **operational data registers** like [RINF](#) and [ERATV](#).

The **ERA CCS TMS ontology** (<https://data-interop.era.europa.eu/era-vocabulary/>) provides a coherent and consistent semantic framework for all data shared or processed in the railway system and is, therefore, a pivotal reference for any data specification in the railway sector. All data models for any specific purpose in the railway domain shall comply with and derive from the ERA ontology. Engineering Data needs to be validated before using it to guarantee conformity with the ERA ontology as well as with engineering rules set out and enforced by the data model (see second figure below). Due to the safety relevance of some configuration data and its based engineering data, the validation tooling needs to fulfil EN 50716 requirements for safety-related software (measures need to be applied according to allocated tool class, such as T2 or T3). EN 50716 will be converted into an IEC and extended towards data

configuration.

Regarding the data processing, a *target picture* is defined, and an implementation path during the *migration* to this target picture is considered:

#### Target Picture:

As ERA CCS TMS ontology is based on RDF, data validation must begin with RDF compatibility. In a second step, engineering rules shall also be validated. Either on an RDF basis with SHACL rules, or, if not possible, by applying dedicated scripts to cover the full complexity of some rules.

The standardisation contribution of the System Pillar is the contribution to the ERA CCS TMS ontology for full coverage of CCS/ TMS use cases (including diagnosis and user interfaces support) and the uptake of validation tooling for RDF and engineering rules as provided on the [Interoperability Test Bed](#).

#### Migration Phase:

A second implementation path is still based on ERA-ontology, but uses derived, ontology-conform databases. This allows early adoption and the connection to existing tools and data storage.

Consequently, as shown in the process overview of UNIFE annual report 2024 (see first figure below), the data preparation process includes data aggregation (e.g. measured/ existing infrastructure data) and engineering to build the set of use-case specific (e.g. ETCS, ATO...) configuration data and the validation against RDF and engineering rules. This process provides configuration data in the structure of the ERA CCS TMS ontology.

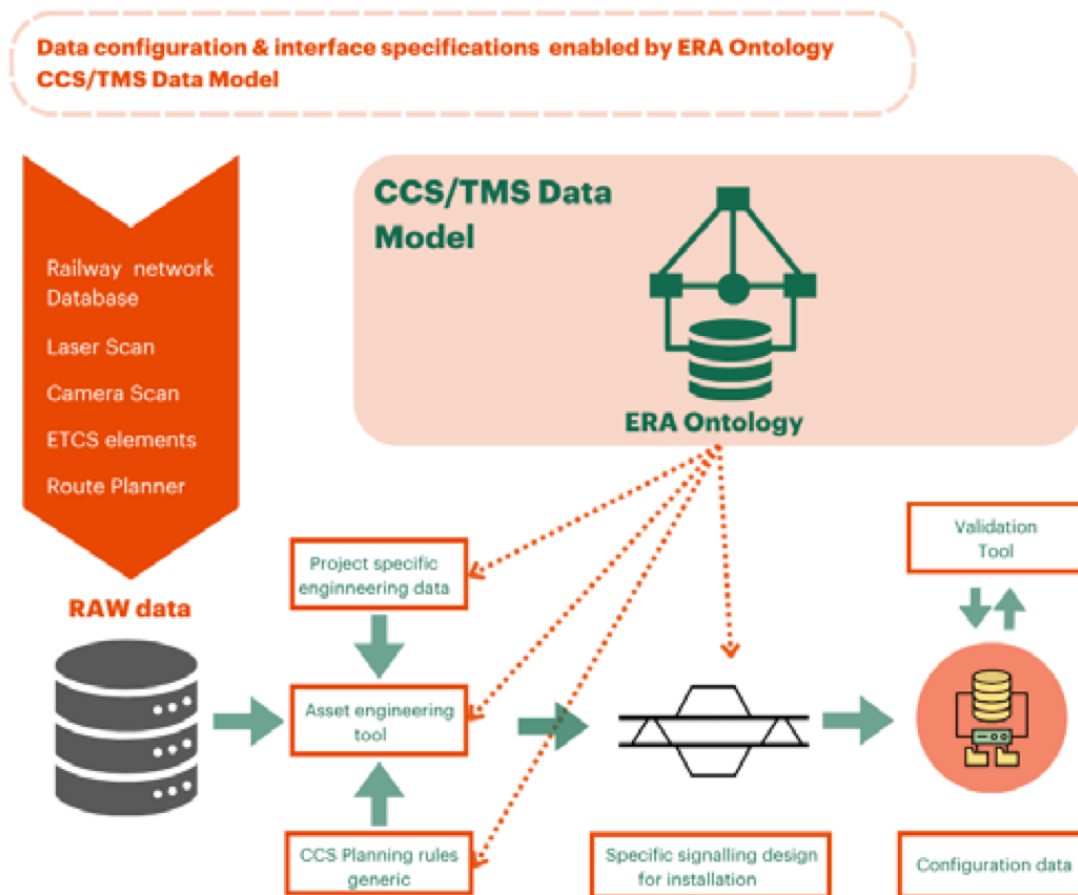


Figure 6 The overall data preparation process: From raw data to validated engineering data, i.e. configuration input data (Source: UNIFE annual report 2024)

[Normal, SPT2TS-131201]

#### RDF

RDF is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ. It supports the evolution of schemas without requiring data consumers to be changed. RDF

extends the linking structure of the Web to use URIs to name the relationship between things as well as the two ends of the link (this is usually referred to as a “triple”). Using this simple model, it allows structured and semi-structured data to be mixed, exposed, and shared across different applications. This linking structure forms a directed, labeled graph, where the edges represent the named link between two resources, represented by the graph nodes. This graph view is the easiest possible mental model for RDF and is often used in easy-to-understand visual explanations (see: <https://www.w3.org/RDF/>) [📄 Normal, SPT2TS-131209 ]

### SHACL

SHACL rules are a way of defining constraints and rules for RDF data. They allow you to specify the structure and content of your data, and to ensure that it meets certain criteria. SHACL rules are expressed in a declarative language, which means that you don't need to write code to use them. SHACL rules are based on the concept of “shapes”. A shape is a template that defines the structure and content of a resource. It specifies the properties that a resource should have, and the values that those properties should take. A shape can also specify constraints on the values of properties, such as minimum and maximum values, or regular expressions that the values must match. See: [https://shacl.dev/article/Introduction\\_to\\_SHACL\\_rules\\_for\\_RDF.html](https://shacl.dev/article/Introduction_to_SHACL_rules_for_RDF.html)) [📄 Normal, SPT2TS-131210 ]

### UNIFE

UNIFE= Union des Industries Ferroviaires Européennes (The European Rail Supply Industry Association) [📄 Normal, SPT2TS-131211 ]

## 4.4 Supplier data configuration

The configuration Data Preparation is followed by Product/Supplier Configuration phase due to the following assumptions:

- It is assumed that the overall configuration data preparation also involves integrating supplier-specific proprietary data parts (e.g., part of OC configuration, software, firmware, etc.), which are not standardised and potentially even not transparent to the Infrastructure Manager.
- In addition, it is assumed that the work split between IM and Supplier can be specific to each IM-Supplier combination.

Therefore, the validated SPT2TS-127778 - Engineering data of Phase 1 must provide a trustworthy source for compiling the final configuration data according to at least partially specific product needs. [📄 Normal, SPT2TS-131191 ]

### Phase 2 – Supplier data configuration

From validated engineering data, the supplier's internal processing creates the product-related

configuration data (E2E phase 2 output):

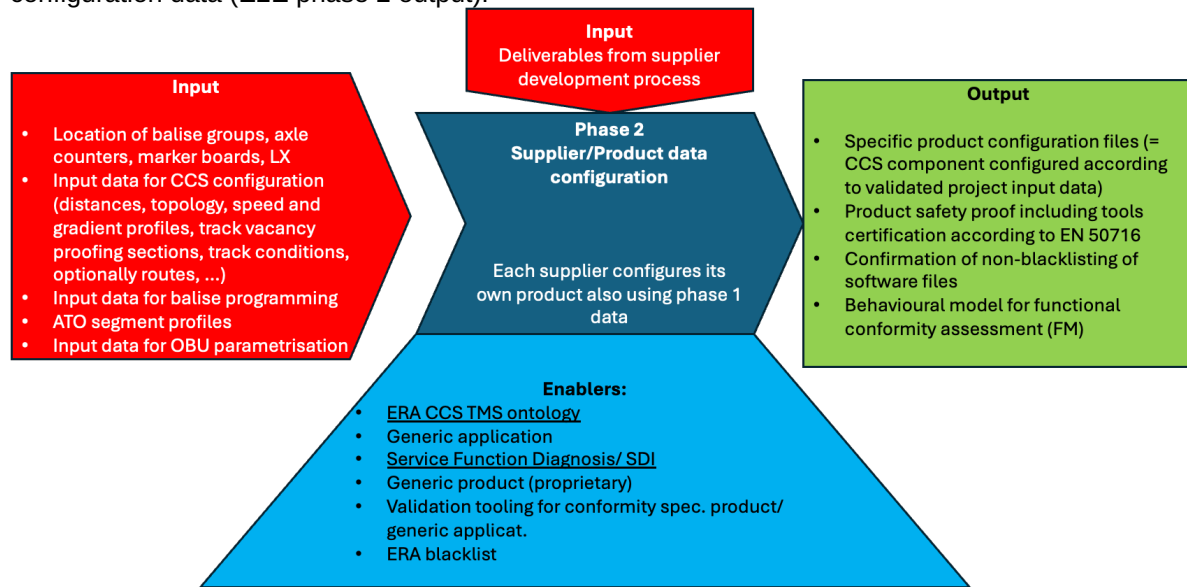



Figure 7 Supplier Data Configuration

#### Links:

- ERA CCS TMS Ontology: [https://gitlab.com/era-europa-eu/public/interoperable-data-programme/era-ontology/era-ontology/-/tree/ext-ccstms?ref\\_type=heads](https://gitlab.com/era-europa-eu/public/interoperable-data-programme/era-ontology/era-ontology/-/tree/ext-ccstms?ref_type=heads)
- Service Function Diagnostics (SDI):  TCCS Service Function Diagnostics (SFD) L5

[📄 Normal, SPT2TS-130975 ]

At the end of Phase 1 and Phase 2, both the engineering data (topology, CCS equipment implementation related data, CCS parameters) and the product design related data (e.g. for the integration and operation of the software in the hardware, data communication enabling processes) require validation:

- Precise, correct and complete engineering data, with EN50716 compliant tool support (E2E phase 1 output)
- Safe and reliable product design (this is validated by conformity with EN 50716), resulting in applicable config data (E2E phase 2 output)

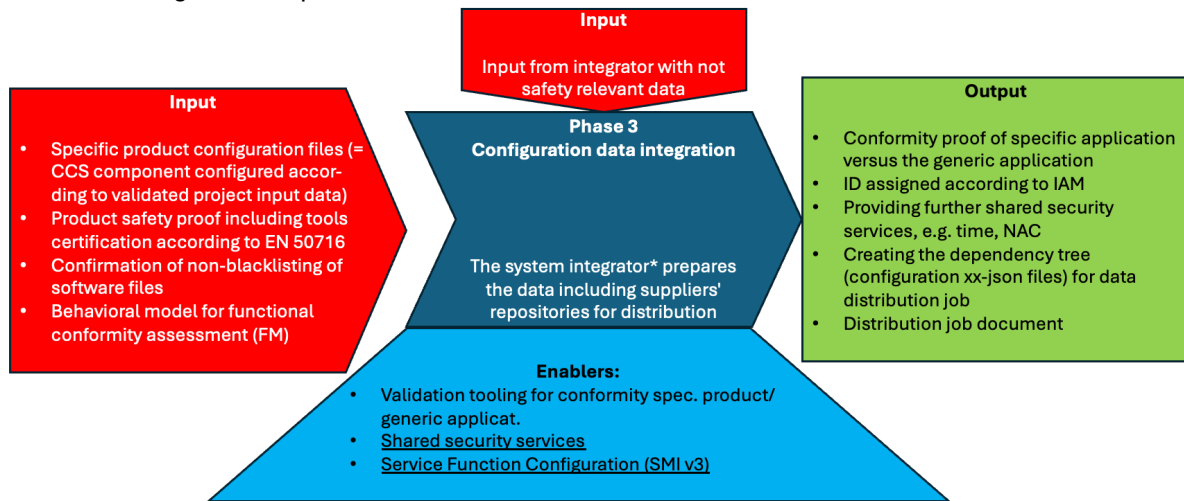
[📄 Normal, SPT2TS-131190 ]

### 4.5 Configuration data integration

#### Phase 3 – Configuration data integration

The product-related configuration data is processed by the system integrator (E2E phase 3 output) and

stored in configuration repositories:



\*can be cascading: A supplier may be integrator of sub-suppliers

Figure 8 Configuration data integration

#### Links:

- Service Function Configuration (SM):  TCCS Service Function Configuration (SFC) L5
- Shared security services: [Cybersecurity specifications](#)

[ Normal, SPT2TS-130973 ]

#### 4.6 Configuration data distribution (SFC)

##### Phase 4 – Configuration data distribution (SFC)

The configuration repositories supply this data when required by the Service Function Configuration (E2E phase 4) for upload on digital components:

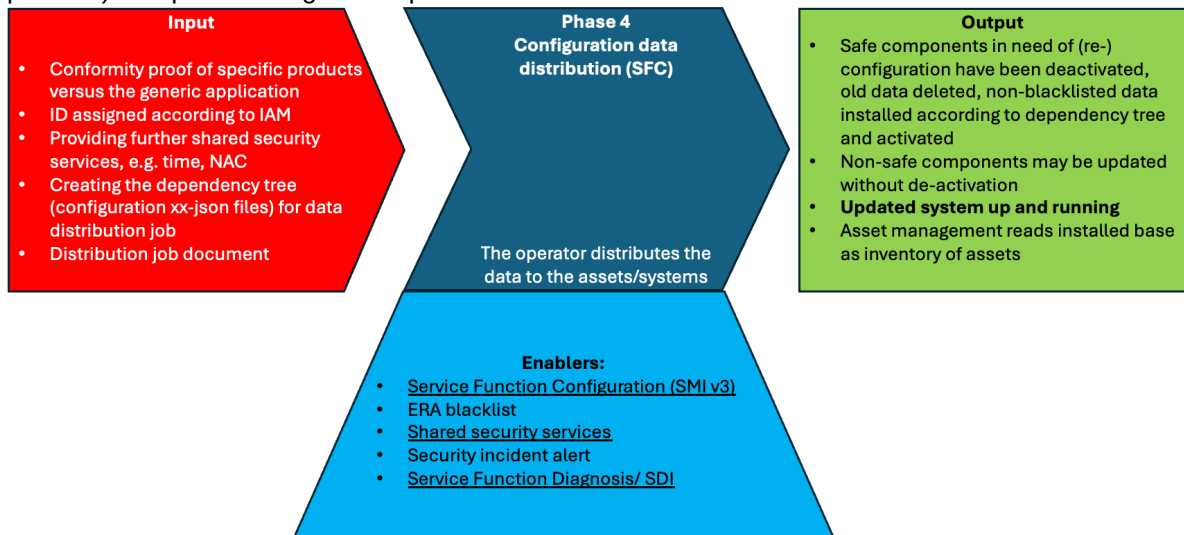


Figure 9 Configuration data distribution (SFC)

#### Links:

- Service Function Configuration (SM):  TCCS Service Function Configuration (SFC) L5

- Shared security services: [Cybersecurity specifications](#)
- Service Function Diagnostics (SDI):  TCCS Service Function Diagnostics (SFD) L5

 Normal, SPT2TS-130971 ]

#### 4.6.1 Problem Statement


The increasing system complexity and supplier diversity in railway environments have exposed significant limitations in current practices for both configuration and diagnostics. Two distinct but interrelated issues emerge:

1. Fragmented and insufficiently validated configuration management, and
2. Heterogeneous and non-interoperable diagnostic approaches.

##### Configuration Limitations

The current standard interface for configuration management, such as Standard Management Interface v2 (SMI v2), was designed for trackside field elements. It supports basic file-based uploads. It lacks awareness of interdependencies between components, and does not provide mechanisms for automated versioning, validation, or safety attestation in the SMI interface itself.

Crucially, safety-related verification is handled separately via the Safety-Critical Interface (SCI) using the RASTA protocol (see IEC standard). This results in two distinct data paths—one for configuration upload and one for validation—creating procedural complexity, operational coupling, and limiting applicability to trackside assets.

Furthermore, SMI v2 does not support dynamic scaling or orchestration across heterogeneous assets. Without dependency resolution or centralised coordination, updates to multiple elements must be performed manually and sequentially, increasing the risk of misconfiguration and operational delays. 

Normal, SPT2TS-131203 ]

#### 4.6.2 Configuration Interfaces and Standards

Historically, configuration management in railway systems has been fragmented across multiple interfaces and standards. The Standard Management Interface v2 (SMI v2), developed by the [EULYNX](#) consortium, supports file-based uploads for configuration data but lacks built-in dependency management, rollback capabilities, or integrated safety mechanisms (EULYNX Consortium, 2023). Safety-critical verification is instead handled separately via the System Configuration Interface (SCI), which relies on the RASTA protocol. This separation introduces operational complexity, limits automation, and restricts the applicability of the interface to field elements only.

The IEC 62853 standard provides a framework for Automated Configuration Management (ACM), primarily for Train Control and Management Systems (TCMS). It introduces principles such as immutable configuration artifacts, recursive dependency validation, and artifact signature verification (IEC, 2018). However, it is focused on onboard systems and does not extend directly to trackside infrastructure or multi-supplier integration scenarios.

At the system level, EN 50126-1 defines the RAMS process and emphasises the need for structured configuration validation as part of demonstrating system safety (CENELEC, 2017). Similarly, EN 50716:2024 defines software lifecycle requirements for safety-critical railway systems, requiring deterministic and auditable software and data configuration processes (CENELEC, 2011; CENELEC, 2017).

In other domains, such as automotive and industrial automation, configuration frameworks are more advanced:

- The Uptane framework in automotive enables secure over-the-air updates of vehicle control units, combining dependency-aware rollout strategies with signed configuration metadata (Kuppusamy et al., 2020).
- In industrial automation, the IEC 62443 family of standards enforces version-controlled, authenticated software and configuration updates across heterogeneous networks (IEC, 2010–2022).
- The ARINC 665 series in aviation specifies file-based configuration management for avionics software, including signature-based validation and aircraft-tail-specific delivery. These external standards demonstrate the feasibility and necessity of integrated, security-compliant configuration management for large-scale, heterogeneous systems. However, their domain-specific constraints limit their direct applicability to railway systems. The need for a unified and scalable configuration interface—capable of

managing both safety-critical and non-safety-critical systems across trackside and onboard domains—remains unmet within current railway practice. [🟡 Normal, SPT2TS-131202 ]

### 4.6.3 Solution Approach

For both Service Functions, a top-down approach is followed across the various system levels, in line with the System Engineering Management Plan (SEMP) process. Several operational user stories illustrating this approach are outlined in the problem statement chapter. In particular, system levels 3 and 4 serve to coordinate efforts between different domains of the railway system, ensuring cross-domain compatibility and integration.

#### 4.6.3.1 Service Function Configuration

The proposed configuration solution approach is centered around the Service Function Configuration (SFC), which consolidates the core functionalities required for configuration deployment and is designed to be basic integrity. All BuildingBlockConfigurations (BBCs) are stored in and retrieved from, a centralised configuration repository. The SMI v3 interface connects the Service Function Configuration with the BuildingBlocks, which may host multiple BBCs, and unifies configuration deployment and safety attestation into a single, standardised interface.

For safety-relevant BBCs, attestation is supported by the Safe Configuration Authority (SCA). The functions performed by the SCA are assigned to Safety Integrity Levels (SILs) in accordance with their criticality. To minimise the system's overall safety footprint, safety-critical logic is isolated and encapsulated within the SCA, ensuring that the remainder of the system remains outside the scope of safety certification.

The following figure provides an overview of the architectural components and their responsibilities:

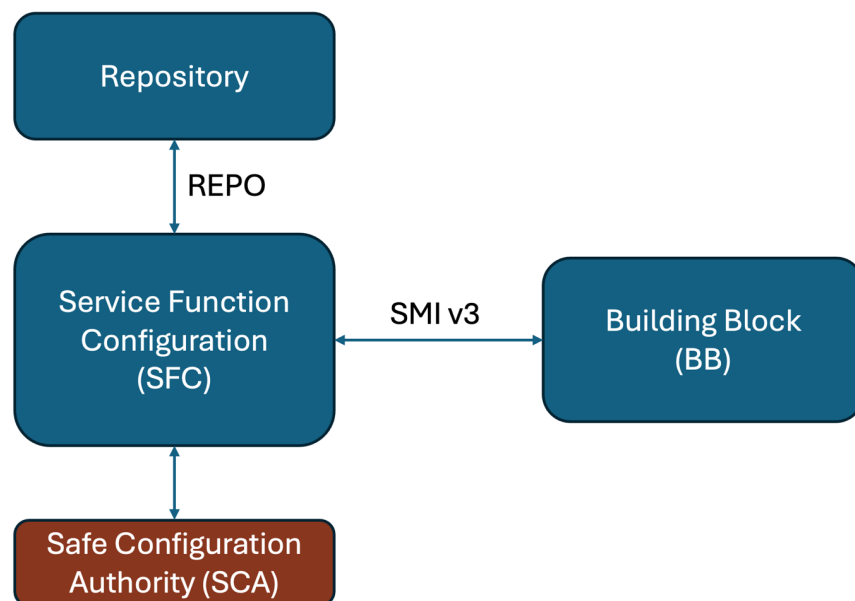


Figure 10 The Service Function Configuration architectural components

#### 4.6.3.2 The Role of SMI v3

SMI v3 acts as the unified interface for managing software and data configurations across all service functions. It integrates configuration artifact retrieval, version control, dependency resolution, and operational readiness checks into a data-driven process that minimises manual intervention. [🟡 Normal, SPT2TS-131204 ]



#### 4.6.3.3 Dependency Management Across Field Elements and Control Systems

Configurations are managed as a dependency tree of Building Block Configurations (BBCs). The top-level BBC acts as the root node and represents a release version for the system. Dependencies can span across multiple system layers—such as interlockings, Radio Block Centers (RBCs), and field elements — and are both versioned and validated recursively. This structure enables selective updates, ensuring that only those BBCs with version changes are deployed, while maintaining consistency and traceability. Recursive validation guarantees that all dependent BBCs are verified before activation, preventing the deployment of incomplete or incompatible configurations. The configuration process consists of the steps: validation, preload, deactivation (applicable only to safe BBCs), activation, and commit.

1. **Validation:** The system verifies the integrity of BBC configuration files using cryptographic hashes. For safety-critical configurations, the entire dependency tree is secured by aggregating protected hashes in a bottom-up manner. This ensures that each configuration level is cryptographically linked to its dependencies. The Safe Configuration Authority (SCA) performs bottom-up verification to guarantee that no subordinate configuration can be altered without requiring a new signature from the responsible integrator at the next higher level. This mechanism enforces end-to-end integrity and traceability throughout the configuration chain.
2. **Preload:** The BBCs configuration files (e.g., configuration, configurationSafe, payloads) are retrieved from a secure repository and prepared for deployment.
3. **Operation interruption:** For safety-critical BBCs, all BBCs that are incompatible with the upcoming release must explicitly interrupt operation prior to deployment. This ensures that no conflicting or outdated BBCs remain active, preventing unsafe system states. In contrast, non-safety-critical BBCs are exempt from this strict operation interruption requirement, allowing for flexible, on-the-fly updates and minimising operational disruption.
4. **Activation:** the new BBC versions are installed bottom up. During this process, Basic Data identifiers are read, and post-installation hashes are computed. Both are transferred for validation in the next step.
5. **Commit:** After activation, for safe BBCs, the Safe Configuration Authority (SCA) performs a final validation by verifying the post-installation hashes against the expected values and comparing the expected basic data identifier with the one received from the Building Block. Upon successful verification, the SCA issues OperationTokens, authorising the safe and validated BBC for operational use.

 Normal, SPT2TS-131206 ]

#### 4.6.3.4 Metadata Structures for Distribution and Orchestration


Structured metadata (e.g., manifests, job definitions) describe:

- Target assets and BBCs.
- Dependency and hash references.
- State indicators like PreloadState and ActivationState.



This enables centralised orchestration across thousands of devices with deterministic audit trails.

 Normal, SPT2TS-131205 ]

#### 4.6.3.5 Safety Attestation and Separation of Responsibilities

Only the SCA performs safety-critical validation and issues runtime tokens as described above. Configuration creation and distribution are decoupled from safety attestation, maintaining strict role separation among suppliers, integrators, and operators.  Normal, SPT2TS-131207 ]

#### 4.6.4 Configuration Process Overview

The following sequence summarizes the distribution phase for the  SPT2TS-127779 - Configuration Data over the SMI interface. The sequence is based on the  Logical Concept and Processes associated with Configuration Repository.



Note: this sequence diagram is only a summary for the configuration distribution with focus on the CCS/TMS configuration data use case and the detailed steps are described in the [Logical Concept](#)

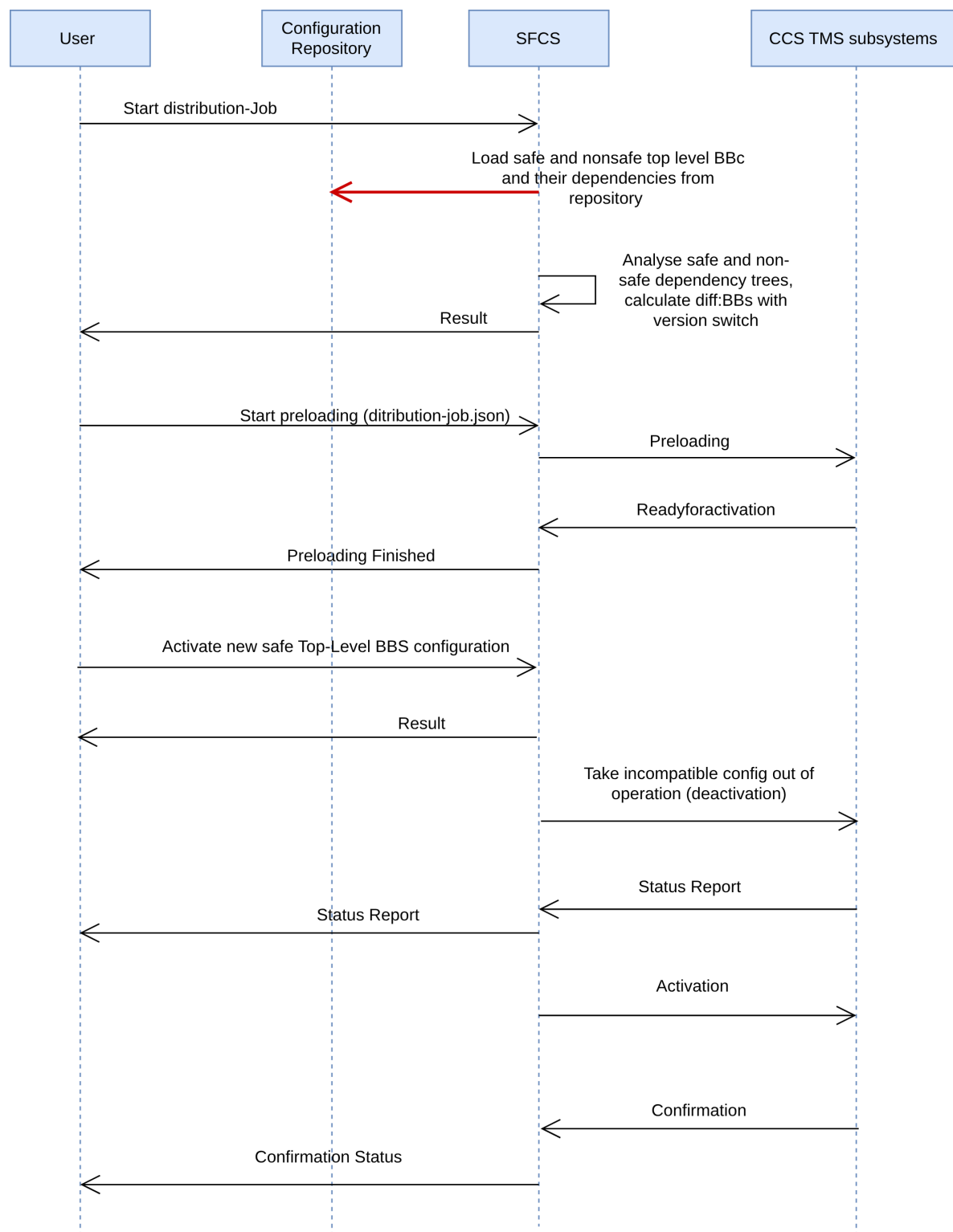




Figure 2 Configuration update sequence associated with Configuration Repository

For the onboard CCS subsystems, the same process is applicable through an onboard

 SPT2TS-128018 - Service Function Configuration System subsystem, which is responsible for the Distribution, Preloading, Activation and Confirmation of configuration data. [ Normal, SPT2TS-129026 ]

#### 4.6.5 Summary

For the initial and subsequent configuration of CCS components for trackside and trains, a configuration management process is proposed. The System Pillar has standardised the secure distribution of safety related and non-safety related configuration data – including topology data and software, e.g. firmware. The dependencies of the configuration are explicitly defined in the form of a “dependency tree”. That is IT proven practice for complex projects, e.g. using Maven or Gradle. A dependency tree represents the hierarchical structure of all the dependencies a system requires. It shows how each configuration item in a specific version depends on other configuration items in a specific version. The configuration items are stored in a Configuration Repository that is capable of resolving and downloading transitive dependencies in other Configuration Repositories. Managing dependencies can become complex, especially in large systems. The dependency tree helps to visualise these relationships and to identify configuration items that have a version change when a new top-level version is chosen for distribution, including potential conflicts. The data-driven and non-safe configuration interface is called SMI – Standard Maintenance Interface. SMIs enable the distribution of safe and non-safe configuration data according to the dependency tree. The dependency tree is not a result of the data preparation process, needs to be defined by the integrator and is the only way to configure the operational systems consistently.

The figure below shows the continuation of the end-to-end data process from validated engineering data (configuration input data) resulting from the data preparation process and product design related processes as explained above towards the configuration of all affected components. In this process a safe configuration authority (SCA) ensures also a safe configuration process via non safe interfaces (SMI v3).

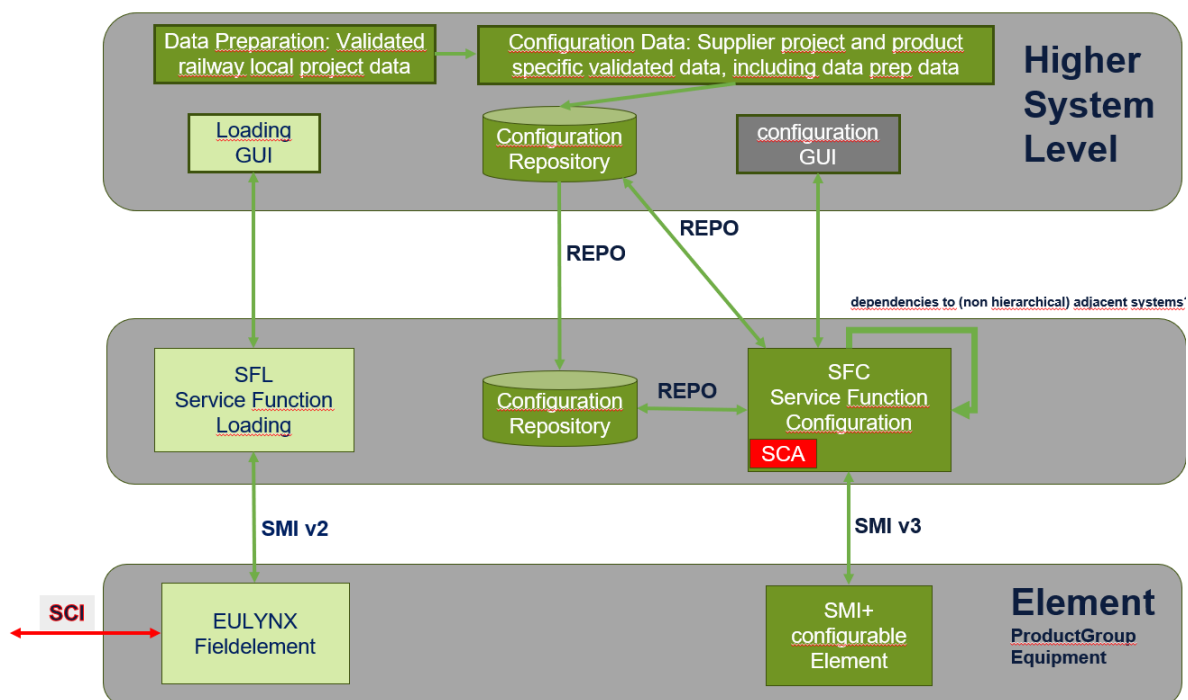


Figure 11 Service Function Configuration (SFC) and legacy predecessor “Service function Loading” (SFL, formerly known as MDM or MDCM). SCA = Safe Configuration Authority, SMI+ = SMI advanced (SMI v3) as standardised by System Pillar (enables configuration of all systems without SCI involvement), SMI = existing EULYNX interface for Service Function Loading (SFL), repo = data repositories

The standardisation contribution of the System Pillar is the standardised configuration process based on OPC-UA standards for data distribution, the specification of the safe configuration authority (SCA) and the application of a dependency tree for selected and validated data configuration.

#### Maven -

Apache Maven is a software project management and comprehension tool. Based on the concept of a project object model (POM). [📄 Normal, SPT2TS-131212 ]

#### Gradle -

Gradle is an open-source build automation tool designed to manage the development process of software projects for building, testing, and deploying applications across various platforms and languages. Gradle builds on the concepts of Apache Ant and Apache Maven, introducing a Groovy and Kotlin-based domain-specific language (DSL) for project configuration, which contrasts with the XML-based configuration used by Maven. It supports multiple programming languages, including Java, Groovy, Kotlin, Scala, C/C++, and JavaScript, see <https://gradle.org/>. [📄 Normal, SPT2TS-131213 ]

### 4.7 Demonstration E2E Process

The E2E data process has been demonstrated in a reference application of the ERA CCS TMS ontology for configuring digital assets. The figure below shows the data, files and tools used. For more details, please see [ERA Rail Data Forum 2025](#).

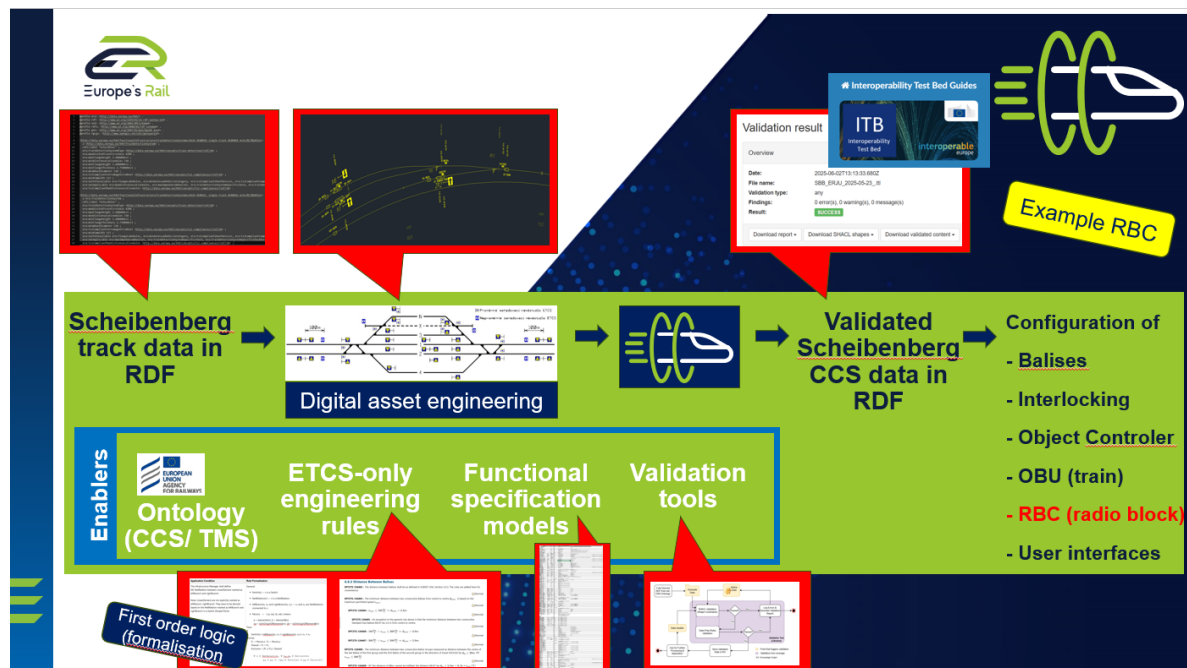


Figure 12 EU test site Scheibenberg full process

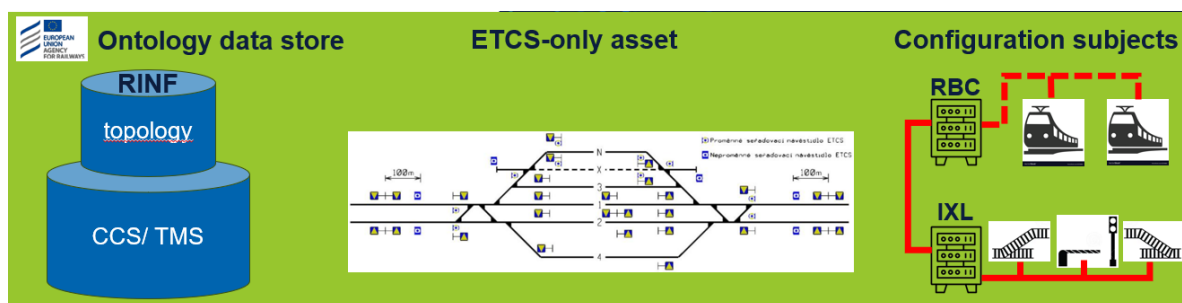


Figure 13 Model, method, tooling and specific project data

CCS/TMS extended ontology file for  
configuration of ETCS L2 in UNISIG  
Subset 026 compliant simulator

Example RBC

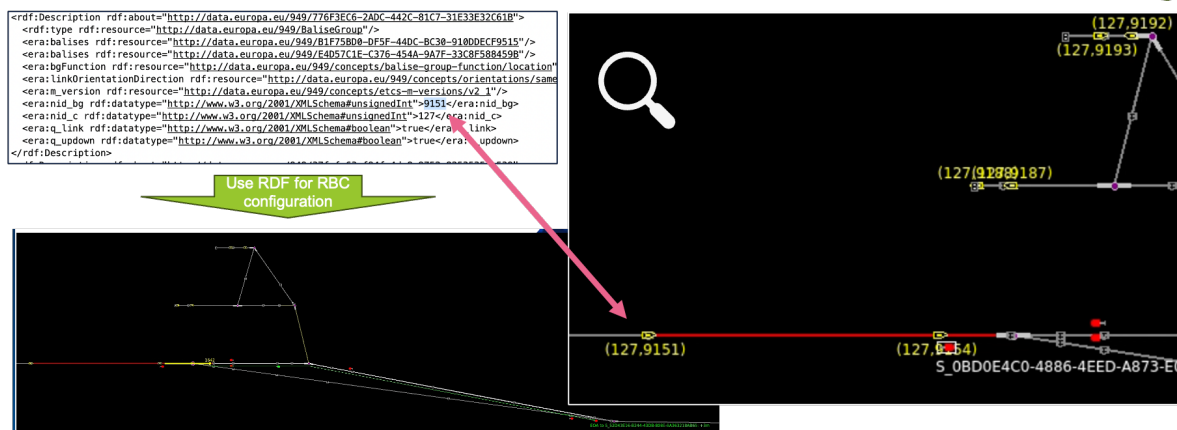


Figure 14 Proof by Simulation: Deriving RBC configuration from RDF files

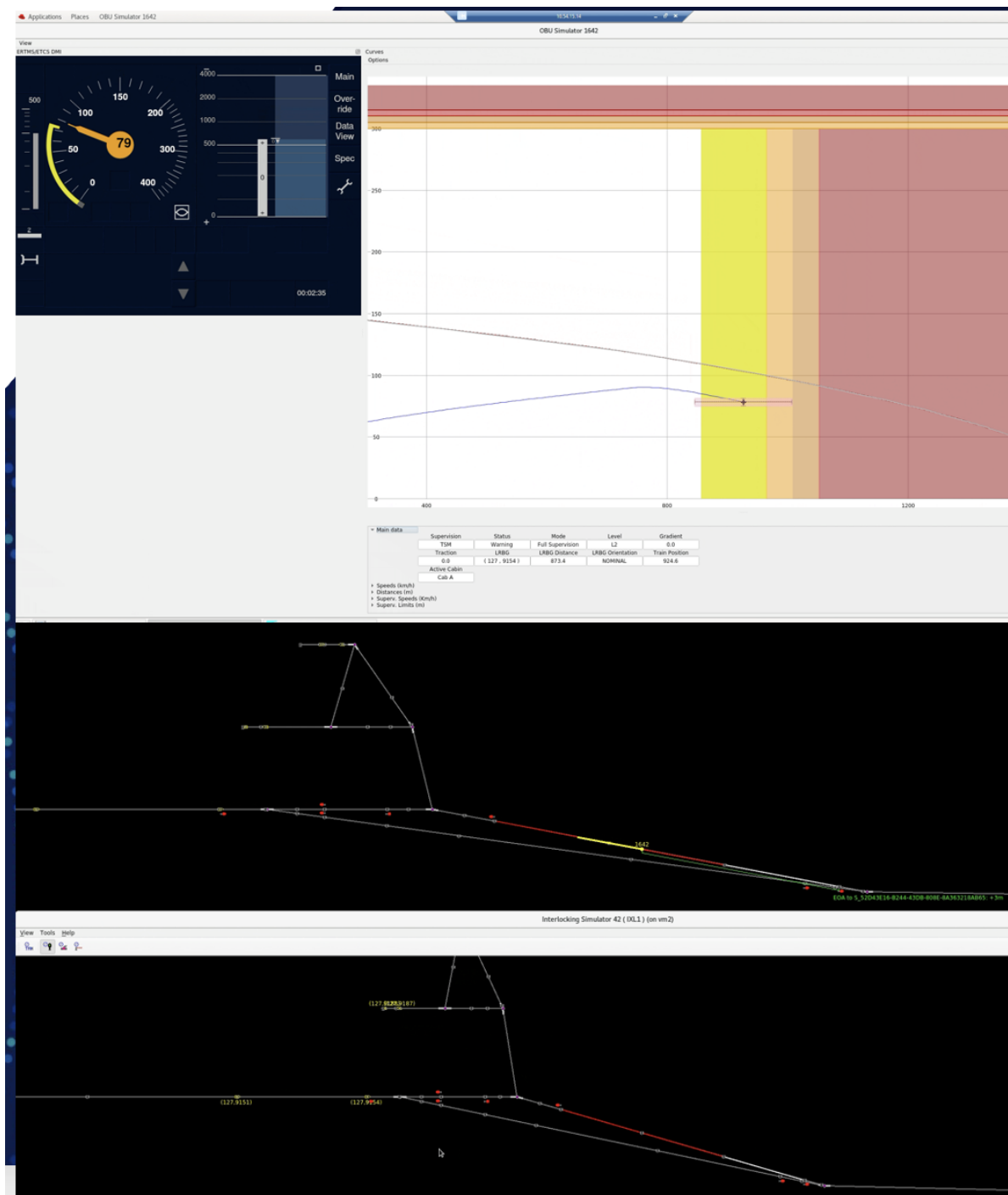


Figure 15 Execute simulation as configured by E2E process

The goal of the implementation is to achieve a first feasibility experience for the generic E2E data preparation process for a CCS subsystem. The chosen subsystem was the configuration of Radio Block Center (RBC) as specified in the subset.

The data prep process begins with the extraction of the relevant CCS information from the extended ERA Ontology. These CCS extracted objects are then populated with the project data (Topology, speed, gradient, geometry etc.) partly extracted from RINF and IM database as well as measurements. These data serve as the basis of the engineering of the trackside assets and parameterization of model contents. The output of the process is a file with all relevant input data for the configuration of a simulator for the RBC.

## 5 Safety

The Evolution Management of Safety-Related Modular Systems process defined by the PRAMS team outlines a structured approach for handling changes, including impact analysis, software development, assessment, and testing. This process is closely connected to the Service Functions Configuration and Diagnostic through attributes defined in the Building Block Configuration, enabling the railway sector (e.g. suppliers, railway understandings) to adopt a standardised method for managing system evolutions. In addition to this, to ensure that the Service Functions Configuration is defined safely, a risk analysis based on the Failure Modes and Effects Analysis (FMEA) is conducted at system level 5. This analysis guarantees that both data preparation and service function configuration are safely managed. Finally, PRAMS (Performance, Reliability, Availability, Maintainability, and Safety) requirements are established for data preparation, update management and service function configuration, reinforcing the overall integrity and robustness of the system. [🟡 Normal, SPT2TS-131208 ]

## 6 Security

Security services, including a secure time distribution service are shared via SSI. In case fixing an IT-security issue requires a new configuration download of affected sub-systems, SMI comes into play. An example is OPC-UA server requesting via SSI from IAM, which roles the login user has - and what it is allowed to configure insulated (see [EU-Rail Cybersecurity Specifications](#)).

Independent from the currently 9 SSI shared services, IT-security is ensured for any data communication according to IT-security standards (EN ISO 27000, EN IEC 62443, EN IEC 63452).

### IAM-

IAM (identity and access management) gives secure access to resources—like emails, databases, data, and applications—to verified entities, ideally with a bare minimum of interference. The goal is to manage access so that the right people can do their jobs and the wrong people, like hackers, are denied entry. The need for secure access includes contractors, vendors, business partners, and people working on personal devices. IAM makes sure that each person who should have access has the right level of access at the right time on the right machine. Because of this, and the role it plays in an organisation's cybersecurity, IAM is a vital part of modern IT. [🟡 Normal, SPT2TS-131214 ]

## 7 Is the system running well and how will it do? Diagnostics will tell- if it can!

### 7.1 Diagnostics Limitations

Diagnostic processes in current railway systems are often fragmented, proprietary, and lack semantic interoperability. This hinders timely fault detection, efficient maintenance, and strategic asset planning across diverse roles and organisational levels.

#### 7.1.1 Operational Limitations

Operators and maintainers are often unable to access real-time and standardised diagnostic data, leading to delayed fault response and poor situational awareness. Maintenance staff must rely on vendor-specific tools and documentation, making it difficult to:

- Understand system status during fault events,
- Identify faulty components (LRUs) with sufficient accuracy, allowing to exchange the faulty component as quick as possible
- Estimate the operational impact of a component failure due to lack of functional dependency models.

Diagnostic procedures are further complicated by inconsistent or outdated inventory information, requiring cross-referencing across disconnected systems (e.g., paper-based plans, Enterprise Resource Planning Systems - ERP, dispatch records). These inefficiencies increase MTTR and error-proneness.

### 7.1.2 Tactical Limitations

Maintenance planners require standardised diagnostic messages and equipment models to shift from scheduled to condition-based maintenance. However, today's diagnostics often lack:

- Consistent semantics across suppliers,
- Fault trend data linked to operating context (e.g., environment, usage),
- Predictive insights for wear reserves or failure forecasts.

Without standard models, planners cannot prioritise fault handling dynamically, assess component survivability, or feed diagnostics reliably into ERP or planning systems.

### 7.1.3 Strategic Limitations

At the strategic level, asset managers need cross-manufacturer diagnostic comparability and historic fault data to support:

- Procurement decisions based on past availability and performance,
- Recall campaigns across reused component types,
- Long-term migration and claim management strategies.

Current vendor-specific implementations do not support systematic dependency analysis, semantic interoperability, or single-source-of-truth integration, limiting organisational learning and strategic optimisation.

### 7.1.4 Need for Standardised Diagnostics

The lack of a harmonised diagnostics framework prevents operators from exploiting the full value of condition data across life-cycle stages. To overcome this, a Standard Diagnostics Interface (SDI) is required that:

- Enables cross-supplier interoperability through a shared semantic model. It is important to note that these models need to be based on or extend the ERA ontology.
- Provides consistent fault localisation, status history, and functional dependencies,
- Integrates with planning, training, and asset management systems through a modular equipment model,
- Supports real-time and historical condition monitoring to enable predictive maintenance and strategic decision-making.

Without such standardisation, diagnostics remain an isolated function—fragmented, reactive, and misaligned with the sector's digital ambitions.

## 7.2 Diagnostics Interfaces and Standards

Several diagnostic interface efforts have emerged in European railway digitalisation, aiming to address the heterogeneity of monitoring systems across suppliers and national operators.

Earlier diagnostics implementations, such as those developed under the German NEUPRO project, introduced structured diagnostics for different trackside components. NEUPRO defined technical message formats and standardised semantic models for equipment, network structure, and product groups—allowing applicability for cross-supplier diagnostics, root cause analysis, and integration into asset management systems. These diagnostic models were later integrated into the EULYNX specifications for trackside assets.

In Europe's Rail the current work is to integrate diagnostics into the EU railway system. On the lower levels the application of artifacts like the equipment model needs to be described further to easily be applied by suppliers. Furthermore, the approach needs to be applicable by all domains. That implies a common diagnostic meta data model and an easy-to-use toolchain to produce the descriptions and models for:

- Generic diagnostic elements (e.g., sensors, network components),
- Product-group specific models (e.g., switches, IO devices, door systems),
- Equipment structure and topological dependencies.



This standardisation allows real-time condition monitoring and supports structured analysis, such as fault isolation, impact propagation, and condition-based maintenance planning.

In parallel, the European Union Agency for Railways (ERA) is developing a cross-domain ontology framework to semantically harmonise railway data across systems, operators, and countries. While the ERA initiative does not define specific diagnostics models, its work is highly relevant: the SDI models and semantics are designed to be compatible with ERA's ontology to ensure future interoperability. The ERA ontology aims to:

- Enable cross-border dataset linking and reuse,
- Harmonise railway terminology across member states and systems,
- Support flexible querying without code changes, enabling automation and analytics.

The alignment between SDI's diagnostic modeling and the broader semantic architecture promoted by ERA represents a critical methodological link—ensuring that diagnostic data can be contextualised, queried, and reused across organisational and national boundaries.

### 7.3 Service Function Diagnostics

The Service Function Diagnostics (SFD) framework consolidates diagnostic data across manufacturers and system domains via the Standard Diagnostics Interface (SDI), developed under Europe's Rail. SDI provides a structured, semantically harmonised interface for both real-time and historical diagnostics, supporting operational, tactical, and strategic use cases.

#### 7.3.1 Generic and Product-Specific Models

SDI distinguishes between generic equipment models—which describe the physical structure of components such as controllers, power supplies, network and storage units—and product group-specific models representing logical functions, such as switches, signals, IO devices, and level crossings. These models use both hierarchical references (e.g., HasComponent) and functional dependencies (Implements, Drives, ProvidesPowerTo, etc.) to represent structure and behavior, enabling cause-effect reasoning within complex systems. By modeling functional dependencies explicitly, SDI enables automated root cause analysis and system impact assessment. For example, it becomes possible to infer the operational consequences of a failed controller or the cascade effect of environmental conditions or a failed power supply on dependent components. This supports maintainers, dispatchers, and planners in both incident response and preventive action planning.

#### 7.3.2 Semantic Representation and Toolchain Support

All models are primarily represented in RDF/OWL, establishing a semantic foundation aligned with the European Railway Agency (ERA) ontology. This ontology-first approach ensures that all downstream representations, such as UML class diagrams, attribute lists, and OPC UA NodeSet2 models are systematically derived from the ontology using a metadata-driven toolchain. This guarantees consistency, supports semantic queries, and enables cross-system interoperability through SPARQL-based reasoning at higher abstraction levels.

#### 7.3.3 ERP and System Integration

The SDI model integrates seamlessly with enterprise resource planning (ERP) and maintenance management systems. It supports workflows such as online asset inventory, condition monitoring, fault diagnosis, automated ticket generation, and feedback into maintenance planning. Standardised semantics reduce training effort and ensure consistent asset interpretation across manufacturers.

To enable predictive maintenance, the Service Function Diagnostics integrates not only real-time monitoring data but also historical repair logs, usage context, and environmental factors. These are semantically enriched, allowing cross-operator learning and strategic improvements. Semantic standardisation ensures that failure data, corrective actions, and asset conditions can be reused across systems without redundant modeling or proprietary logic.

#### 7.3.4 Diagnostics Harmonisation and Sector Impact

The Service Function Diagnostics creates a harmonised diagnostic framework that transcends vendor boundaries. By unifying physical models, product-specific diagnostics, and standard semantics, SDI ensures consistent, vendor independent access to diagnostic information. This supports interoperable



asset management, reduces training and integration costs, and enables international alignment across the European rail sector.

As an important prerequisite for standardised diagnostics, a consistent product group model structure is required. This structure enables domain experts to define and maintain diagnostic models in a modular and scalable way. In the trackside domain, this partitioning has already proven successful and supports effective modeling across different types of equipment.

For other domains—such as rolling stock—a comparable structure must be agreed upon to ensure consistent diagnostics. EN 15380-2, -4 and -5 provide a standardised classification system for rolling stock. It defines a hierarchical structure of product groups, enabling clear categorisation of components and systems. The standard starts with a Main Group (e.g., Vehicle Body, Bogie, Braking System), followed by Sub-Groups and Component Groups, offering granularity down to individual obtainable and replaceable units.

Using this structure as a basis for trainside diagnostics would allow a cross-supplier consistency in how systems like brakes, doors, or HVAC units are represented. This would allow to reuse diagnostic logic across different vehicle types and fleets.

## 7.4 Summary

Diagnostic data can only be effectively used if its semantics (meaning) are standardised and a process of collecting, processing and aggregating for diagnostic data users is in place. A digital twin of the system is provided to the asset management by assembling the related models. The **digital twin** models of the subsystems consist of both a **physical** and a **logical** model:

- The **physical** model is a modular building block system that enables suppliers to describe their specific physical architectures in a standardised way. This ensures that maintenance teams can identify the correct spare part when a replaceable unit (LRU) fails.
- The **logical** model collects data relevant to a specific product group from an operational perspective, helping to determine whether production can continue. Examples of such models include the EU-RAIL Trackside Assets SP/EULYNX SDI product group models for switches, IO devices, and TVPs.

These two models are linked through references that establish connections, such as which physical device implements which logical function or which power supply provides energy to which components. These functional references are essential for root cause analysis, allowing maintenance teams to prioritise repairs efficiently. These models standardise the semantics while allowing suppliers to extend them to accommodate their specific needs. This standardisation is crucial for ensuring interoperability of diagnostic data. However, not all diagnostic data is openly accessible: According to EU regulations (EU Data Act), railway operators (RU and IM) own the data generated by their assets, regardless of the supplier. It is up to the data owner to share on a voluntary basis. Also, non-standardised data points in components provide data that may not be usable for anybody else than the component supplier.

Data collection and processing are enabled and facilitated by OPC-UA and its associated services.

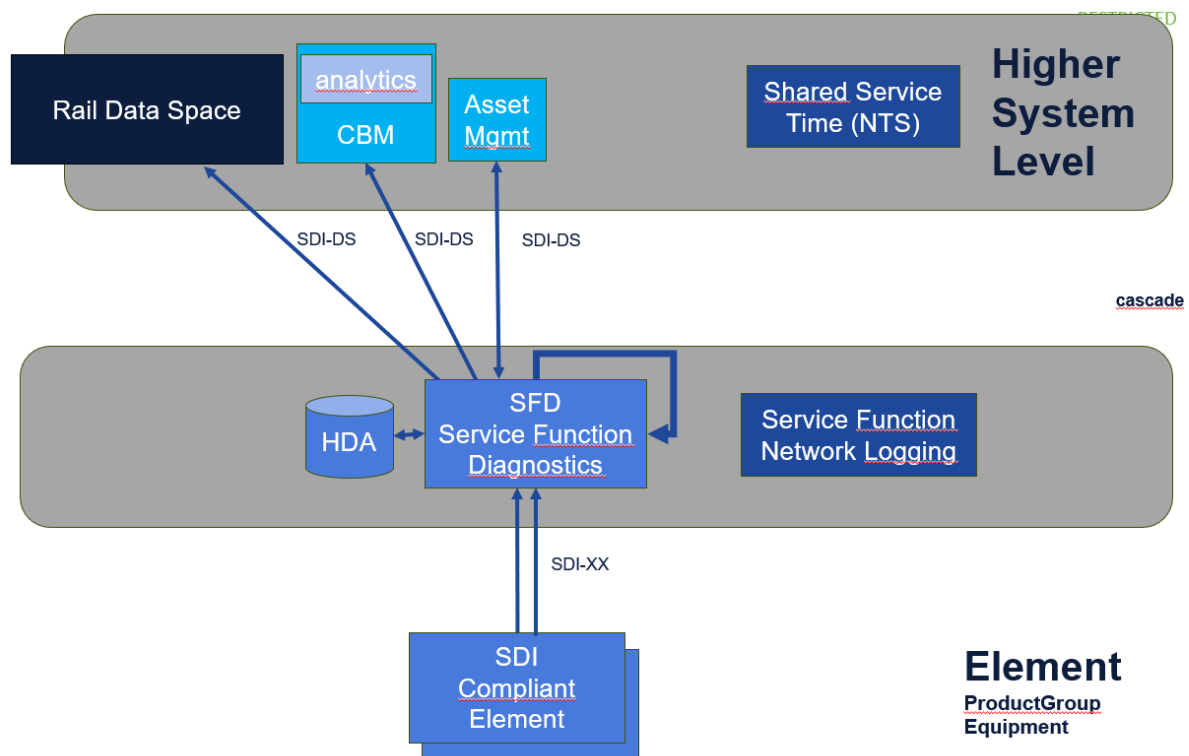


Figure 14 Service Function Diagnostics (SFD). Formerly known as MDM or MDCM (CBM = Condition Based Maintenance, HDA = Historian Data Access)

OPC-UA is used to collect and manage diagnostic data within the assets of a railway operator. It serves as the interface to the “single source of truth” by reading data directly from installed assets: The installed base is the “single source of truth”. When a spare part is replaced, OPC UA ensures that the asset management system is updated accordingly. The asset management system needs to be aware of the new component (like IAM, NAC) before the new asset is introduced in the system.

For selective and controlled sharing of diagnostic data with external stakeholders, such as product suppliers, the European Rail Data Space provides a defined framework. Under the umbrella of the International Data Spaces Association (IDSA), the EU Rail Data Space offers connectors, reference contracts, and services to facilitate voluntary data exchange between partners based on bilateral agreements.

The standardisation contribution of the System Pillar is the standardised diagnosis process based on OPC-UA standards for data collection, product group models for data points standardisation and data sharing services like GS I or Data Spaces.

### Product Group -

group of related products which share some common attributes like features, use, production processes etc. Many product groups combine to make a product line. See: <https://www.mbaskool.com/business-concepts/marketing-and-strategy-terms/11951-product-group> [Normal, SPT2TS-131215]

### IO -

Single-drop digital communication interface for small sensors and actuators. The Subsystem - Generic IO is used for integrating signaling components, particularly in the track and platform area, which are controlled or monitored with input and output information.

[Normal, SPT2TS-131216]

**TVPs -**

Track vacancy proving: The function which proves that a defined section of track is vacant. [📄 Normal, SPT2TS-131217 ]

**RU -**

RU = Railway Undertaking, see also [https://www.era.europa.eu/system/files/2022-11/era\\_technical\\_document\\_tap\\_b\\_8\\_v1.2.pdf](https://www.era.europa.eu/system/files/2022-11/era_technical_document_tap_b_8_v1.2.pdf) [📄 Normal, SPT2TS-131218 ]

**IM -**

IM = Infrastructure Manager, see also [https://www.era.europa.eu/system/files/2022-11/era\\_technical\\_document\\_tap\\_b\\_8\\_v1.2.pdf](https://www.era.europa.eu/system/files/2022-11/era_technical_document_tap_b_8_v1.2.pdf) [📄 Normal, SPT2TS-131219 ]

**OPC-UA -**

OPC Unified Architecture (OPC UA) is a cross-platform, open-source, IEC62541 standard for data exchange from sensors to cloud applications. It provided multiple services: Concepts, Security Model, Address Space Model, Services, Information Model, Mappings, Profiles, Data Access, Alarms and Conditions, Programs, Historical Access, Discovery and Global Services, Aggregates, PubSub, Safety, State Machines, Alias Names, Role-Based Security, Dictionary Reference, File Transfer, Device Onboarding, Base Network Model, Common Reference Types, Scheduler. [📄 Normal, SPT2TS-131220 ]

## 8 OPC-UA for communicating Diagnostic Data

### 8.1 Structured Information Models

OPC UA supports fully structured, namespace-based information models. Each supplier or domain can define its own namespace while inheriting from standard types, allowing:

- Modular and extensible equipment and function models,
- Supplier-specific extensions without breaking interoperability,
- Formal modeling of component hierarchies and behaviors.

This modular approach enables both standardisation (for interoperability) and customisation (for vendor-specific features) in the form of companion specifications.

### 8.2 Hierarchical and Functional References

OPC UA supports a wide range of reference types, including:

- Hierarchical references (e.g., HasComponent, Organises) to describe physical decomposition,
- Functional references to model non-hierarchical dependencies and logical relations (e.g., “output function depends on sensor input”).

This capability is essential for diagnostic root cause analysis, impact assessment, and modeling the functional dependencies required for predictive maintenance and safety assessment. It is possible to define custom references.

### 8.3 Semantic Integration and Historical Access

This graph structure closely resembles semantic web technologies such as RDF (Resource Description Framework) and OWL (Web Ontology Language). As a result, OPC UA models—especially those defined in NodeSet2 XML format—can be systematically transformed or aligned with RDF/OWL-based triplestores, enabling integration with higher-level semantic models like the ERA ontology. This interoperability allows domain-specific diagnostic models (e.g., for switches, I/O devices, or controllers) to be semantically linked to asset lifecycle, topology, and repair information across system boundaries.

### 8.4 Historical Data and Event Integration

OPC UA offers native support for both historical data access and event-driven communication. OPC UA allows time-series data from sensors, components, and system states to be stored and retrieved in a standardised manner. This enables maintenance planners and analysts to track the evolution of asset behavior, correlate past failures with environmental or operational conditions, and support longterm

performance assessments. Historical data is essential for predictive maintenance and supports lifecycle documentation, such as MTBF calculations and failure rate analyses. OPC UA provides a flexible mechanism for event generation, subscription, and alarm handling. Repeatable events like turning a switch, starting up a device can be modeled as an OPC UA event. Events can also be used for tracking follow ups to fault states.

### 8.5 Built-In Features for Secure and Scalable Operation

Key runtime features include efficient real-time data monitoring via subscriptions with dynamic configuration at runtime, and method calls that allow clients to trigger commands or queries on the model (e.g., start diagnostic routines or validate configurations). A fine-grained role and permission model controls data access and runtime interaction—especially important for restricting sensitive method calls to authorised roles only. While methods are forbidden in the SDI interfaces, they are very important in the SMI v3 model.

### 8.6 Communication Protocol and SDK Support

OPC UA natively supports binary encoding for efficient data transmission and has built-in security mechanisms including signing, encryption, authentication, and reverse connect, which is particularly useful in restrictive railway IT environments.

Its adoption is further facilitated by mature SDKs from multiple vendors (e.g., Unified Automation, Prosys OPC UA, open62541), enabling fast and reliable integration into railway diagnostic and configuration platforms.

In summary, OPC UA provides the scalable, secure, and semantically rich foundation required for the diagnostic and configuration processes in modern, digital railway systems. It supports the modeling, real-time data access, historical analysis, and standardised interoperability necessary for efficient operation, maintenance, and safety management—across suppliers.

Although OPC UA is widely regarded as a comprehensive technology stack that seamlessly integrates key requirements, there is ongoing debate—particularly from the trainside domain—about whether using specialised protocols for individual tasks (e.g., AMQP for messaging, HTTPS for transfer, or separate frameworks for syntax and semantics) might be more efficient. While such a multi-protocol approach can simplify initial implementation, it risks increasing integration complexity and lifecycle costs over the asset's operational lifetime.

note: An **SDK (Software Development Kit)** is a collection of tools, libraries, documentation, and sample code that developers use to create applications for specific platforms, frameworks, or devices. It simplifies and accelerates the development process by providing pre-built components and resources tailored to the target environment.

## 9 Catalogue of Symbols: The Europeaniser for railway staff

Railway staff needs standardised user interfaces for a standardised ETCS-only implementation in Europe, specific to each user group and fully standardised within each user group. The precise user requirements at user interfaces are specified by the mission-critical domains like OD, Traffic CS, Train CS and TMS and will be delivered in line with the harmonised operational rulebook as specified in the System Pillar. Visualisation is based on the single source of truth: The ERA-ontology offers a growing number of concepts for the railway industry and different data models are being derived from it to serve various use cases.

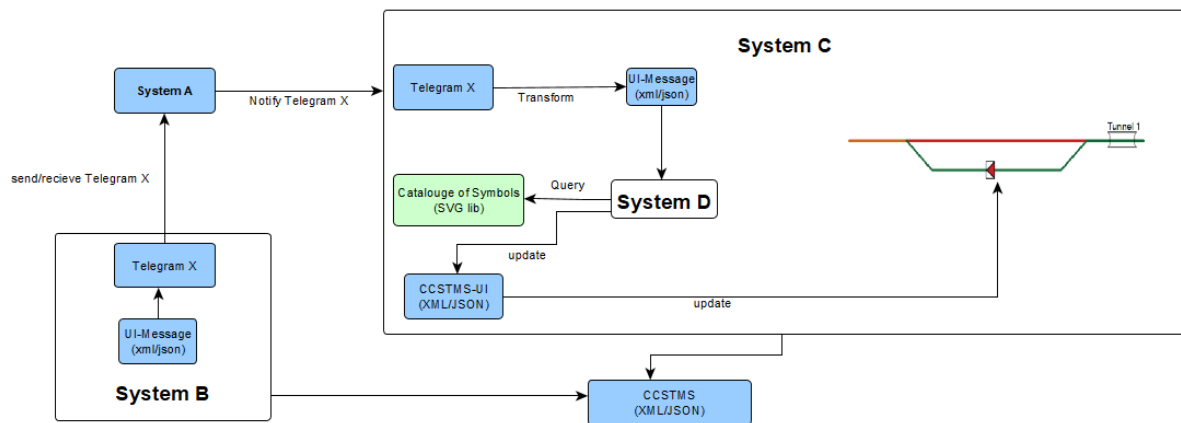
The Catalogue of Symbols is built on the ERA-ontology and is to expand per application through the continuous development of visualisation concepts based on user contributions and needs. As the ERA-ontology is flexible to expand, a back-propagation approach can be applied upon request. This approach ensures that standardisation concepts remain clear and based on standardised terminologies.

The Catalogue of Symbols addresses not only the standardisation of the visual aspects of assets but also their dynamic operations, if applicable. Hence, the Catalogue of Symbols is not only linked to object names but also to their properties and values. A sample use case is the signaling operation screen, where assets change colors and shapes according to their states. The Catalogue of Symbols document can be

considered the user-interface (UI) end use, but it is linked to other documents that ensure the required visualisation. These artifacts include:

- **ERA-ontology** for topological and geometrical aspects of tracks and asset locations
- **UI related content of SCI-xx** (XML, JSON), which provides a standard communication specification
- **ERA-ontology-UI extension** for visualisation

The product development approach requires the integration of ERA-ontology in any required available format, as well as the UI extension. Both serve as configuration files for the visualisation system, providing infrastructure information and an initial foundation for visualisation. The ERA-ontology-UI extension is linked to the Catalogue of Symbols through Id references, where the Catalogue of Symbols offers direct mapping between ERA-ontology information and visualisation aspects. The following figure illustrates the levels of information required to achieve the visualisation goal.



[  Normal, SPT2TS-130352 ]

Figure 15 Catalogue of Symbols integration into a visualisation system

Prominent use cases are:

- Driver's route book
- Signalers work station
- Asset managers diagnosis interface
- Driver machine interface
- Remote driver interface
- Signaling engineer's technical documentation

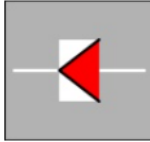
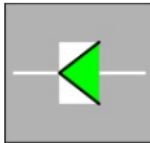
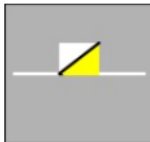
Description	UI-Message	Symbol	SVG file
ETCS Stop Marker Stop	11401.current_status_data=true		Yes
ETCS Stop Marker Go	11401.current_status_data=true and (11401.drive=1 or 11401. drive_and_stop_at_next_signal =true)		Yes
	11401.current_status_data=true and 11401.etc_ma=true		Yes

Figure 16 Extract from the Catalogue of Symbols for standardised representation of information by symbol (SVG file library) and command (SCI-relevant for UI)

Standardised UI are not only vital for standardising operational processes but also key for cost-cutting by preventing product and supplier-specific training costs for railway staff. Furthermore, they significantly contribute to operational safety.

#### Visualisation goal -

Specific attention must be paid to Human and Organisational Factors (HOF), in terms of interfaces and dependencies throughout the lifecycle (with designers, operators, maintainers). See EC Report on preparation of the System Pillar, 20/07/2021, Ares(2021)4674849). [🟡 Normal, SPT2TS-131221 ]

## 10 Reference Implementation

To validate the proposed standardised approach, reference implementations of the Service Function Configuration (SFC), the Service Function Diagnostics (SFD) frameworks and further ERA-ontology related applications like data prep and Catalogue of Symbols have been developed and demonstrated, e.g. at Innotrans and in the CONEMP demo video. These prototypes are not only used to demonstrate the feasibility of data processes including automated configuration and diagnostics but also to serve as a feedback mechanism to refine the ongoing standardisation efforts within Europe's Rail. The implementations help identify missing definitions, ambiguous structures, and practical integration constraints, which are being ported back to the specifications for iterative improvement. As with any mature software standard, reference implementations are indispensable for ensuring practical applicability, consistency, and stakeholder alignment.

The work will be incorporated into upcoming standards on diagnostics and configuration, scheduled for publication in 2027.

## 11 More to come: SERA takes it all!

The creation of the Single European Railway Area (SERA) must not be reduced to merely assembling compatible components. The foundation of this system is built upon the ERA-ontology, shaping a cohesive semantical framework.

Several CCS/TMS use cases, some successfully demonstrated on Innotrans 2024, highlight this transformation:

- Balise Telegram programming
- RBC-Configuration
- Safety logic config
- SCI-XX-Telegrams
- ATO segment profiles generation
- OC-Configuration
- Digital Twin runtime
- IDS-BIM integration
- Cascading Digital registers/ Configuration data repositories for data consumers
- Catalogue of symbols for standardised user interfaces like Driver's Route Book, DMI, Signalers workstation, Maintainers end devices
- Diagnostics (OPC-UA) implementation
- Route Compatibility Check
- Many more applications based on data

The focus is now shifting from specification to implementation, making testing, IT-security and system integration increasingly critical to meeting the needs of railways operations.

Taking railway staff on the digitalisation journey also means a shift on mindset - from "railway data" to "data for railway". Scalable, affordable, industrialised, modular, and maintainable solutions must take precedence over expensive, bespoke, tailor-made systems with uncertain IM-supplier dependencies and proprietary solutions.

With ETCS-only, the radio-based ETCS without signals, a fully harmonised operational, safety and engineering framework becomes reality for the first time in history. Not even one single national rule can any longer be justified! SERA can come! Constraining ETCS with lineside signaling means in contrary to combine the constraints of light signals with the constraints of ETCS: Combining the worst disadvantages of both worlds!

EU-RAIL is fully committed to promoting ETCS-only and ensuring all necessary enablers are in place. This will be achieved by standardising the EU Railway System, ultimately realising the vision of a fully integrated SERA: **SERA at its best**.

### Proprietary solutions -

System Pillar task is to develop the operational concept(s) and functional system architecture for a genuine integrated European CCS system, supported by a model-based systems architecting & engineering approach, beyond the current specifications in the CCS TSI, with much greater standardisation and much less variation than at present. This integrated CCS system shall on the one hand deliver unrestricted movement of trains, on the other hand, it shall create a single market for rail components. The software and hardware installed on board or trackside should be operated and maintained following principles and standards as used in the IT or industrial automation domain: regular, scheduled updates with pre-tested configurations ensure errors and shortcomings are eliminated, maintaining all the products and system throughout EU in line with the interoperability specifications, with manageable upgrade mechanisms. See EC Report on preparation of the System Pillar, 20/07/2021, Ares(2021)4674849). [🟡 Normal, SPT2TS-131222 ]

## 12 References

- ARINC (n.d.) ARINC Specification 665: Loadable Software Standards. Annapolis, MD, USA: Aeronautical Radio Inc.
- CENELEC (2011) EN 50128:2011 – Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems. Brussels, Belgium: European Committee for Electrotechnical Standardisation.



- CENELEC (2017a) EN 50126-1:2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process. Brussels, Belgium: European Committee for electrotechnical Standardisation.
- CENELEC (2017b) EN 50657:2017 – Railway Applications – Rolling Stock Software. Brussels, Belgium: European Committee for Electrotechnical Standardisation.
- DIN, DIN EN 15380-4:2020-05 – Railway applications – Classification system for railway vehicles – Part 4: Rolling stock characteristics. Berlin: Beuth Verlag, 2020.
- EULYNX Consortium (2023) Interface Definition and Specification SMI Eu.Doc.76 v2.0. Brussels, Belgium. Available at: <https://rail-research.europa.eu> (Accessed: May 2025).
- IEC (2010–2022) IEC 62443 – Industrial Communication Networks – Network and System Security – Industrial Automation and Control Systems Security. Geneva, Switzerland: International Electrotechnical Commission.
- IEC (2018) IEC 62853:2018 – Railway Applications – Automated Configuration Management (ACM) for Train Control and Management Systems (TCMS). Geneva, Switzerland: International Electrotechnical Commission.
- Kuppusamy, T., Balasubramanian, A., Henriques, J. and Teodorescu, M. (2020) 'Securing Over-the-Air Updates with Uptane', Proceedings of the 2020 ACM Workshop on Automotive Cybersecurity (AutoSec '20), New York, USA, 12–20. Available at: <https://doi.org/10.1145/3372455.3391100>.
- IEC ahG 28: Safe transmission protocol
- EN 50716:2024 Railway Applications - Requirements for software development (replaces EN 50128 and EN 50657)

### 13 Annex: Delivery Process

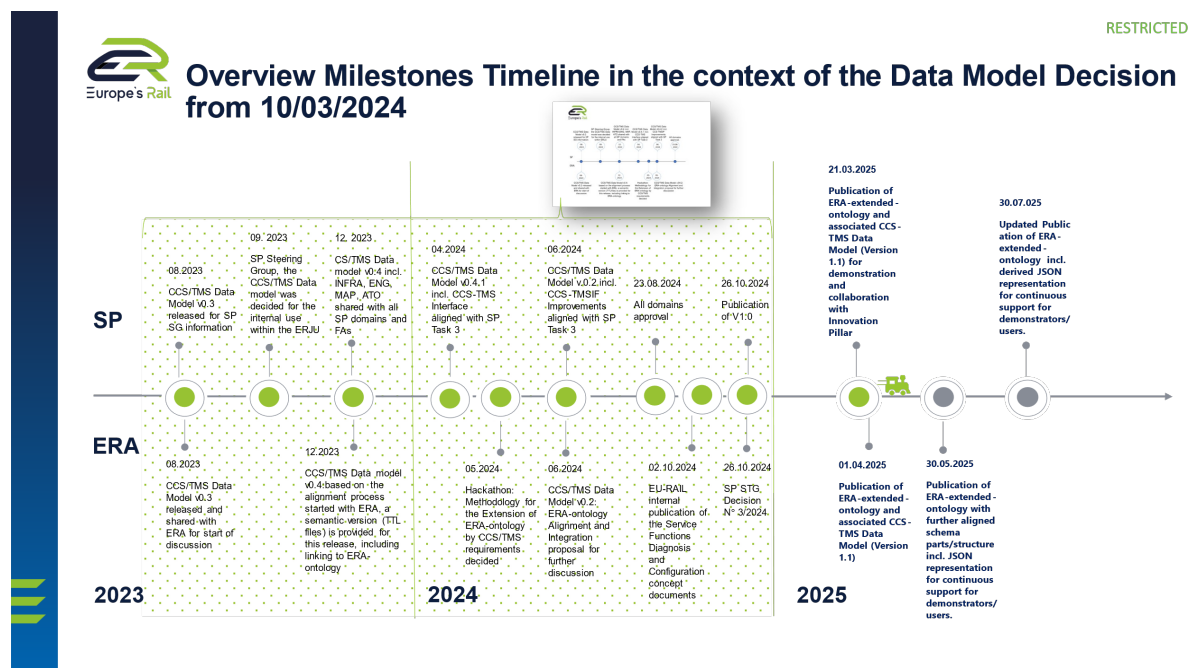


Figure 17 Roadmap from publication of the ERA-extended ontology to SP internal publication of service functions configuration and diagnosis, showing the sector consultation



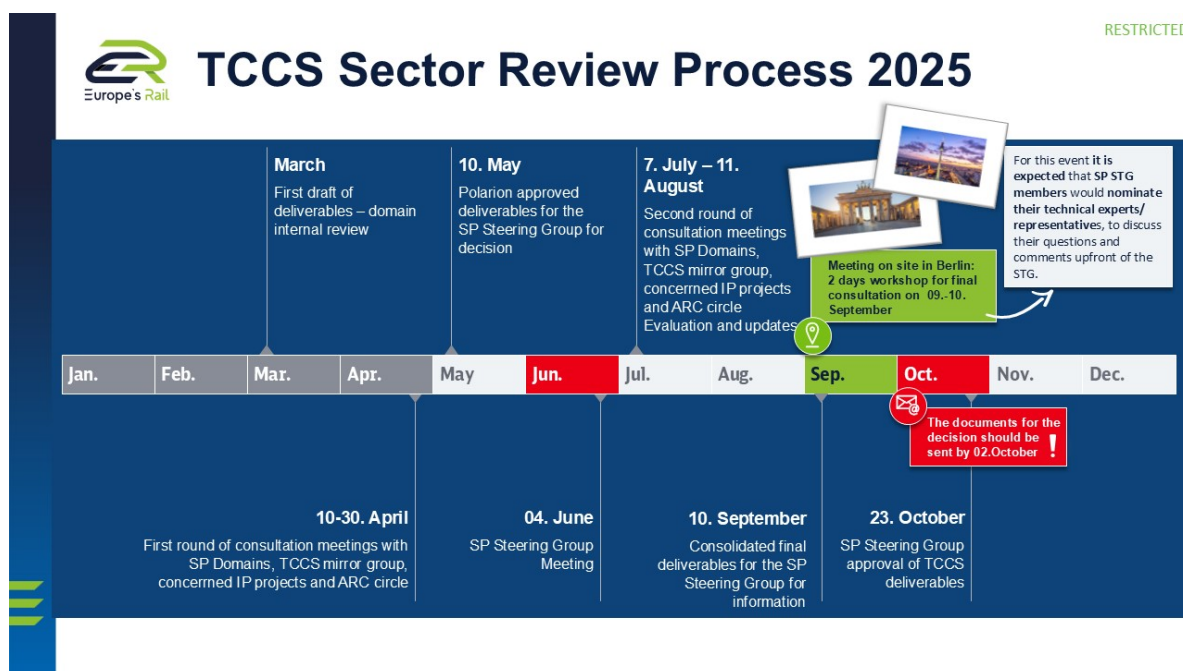


Figure 18 TCCS deliverables consultation and conciliation process 2025 (SC2.4)

RESTRICTED

## First round of consultations with all stakeholders 10.-30. April - completed

Stakeholder:	Date:	Location:	Status:
TACS	17.04.2025	Ms-Teams	Consulted ✓
EET	17.04.2025	Ms-Teams	Consulted ✓
PRAMS	17.04.2025	Ms-Teams	Consulted ✓
SEC	24.04.2025	Ms-Teams	Consulted ✓
ARC	28.04.2025	Ms-Teams	Consulted ✓
OD	28.04.2025	Ms-Teams	Consulted ✓
TCS	28.04.2025	Ms-Teams	Consulted ✓
HD	29.04.2025	Ms-Teams	Consulted ✓
CE	29.04.2025	Ms-Teams	Consulted ✓
TMS/ CM	30.04.2025	Ms-Teams	Consulted ✓
DAC/ FDFTO	30.04.2025	Ms-Teams	Consulted ✓
TCS	30.04.2025	Ms-Teams	Consulted ✓
TCCS Mirror Group	30.04.2025	Ms-Teams	Consulted ✓
Architecture Circle	30.04.2025	Ms-Teams	Consulted ✓
<b>+ Bonus:</b> Associations and SRG	05.05.2025	Ms-Teams	Consulted ✓

**DOMAINS** (represented by a person icon)

**GROUPS** (represented by a group icon)

**Feedback!**

**+ Comments!**

**+ Comments!**

**+ Regular exchange!**

**+ Regular exchange!**

Figure 19 TCCS deliverables first round consultations 2025 (SC2.4)