System Architecture Description

Smartrail 4.0 Architecture

Document Properties

Status: ✔ **document signed**

Version: **1**

Owner: Kuhn Markus (I-SR40-PMO-PLP)

Contributors: Kuhn Markus (I-SR40-PMO-PLP)

Document history

Version (revision)	Changes	Document Owner	Approved	Signed
1 (320982)	1 Update for KB	Kuhn Markus (I-SR40-PMO-PLP)	Schmidt Steffen (I-SR40-STW)	✔ Kuhn Markus (I-SR40-PMO-PLP) Author ✔ Schmidt Steffen (I-SR40-STW) Approver

Abstract

This System Architecture defines the smartrail 4.0 system structure that was developed according to the specific criteria for decomposition, which includes separating according to the expected lifecycle, the safety relatedness and the required availability. The structure contains trackside, on-board and in data-center centralized components for planning and controlling the movement and trackside construction work. Most of the functionality is realized in software and runs on platforms.

Content

1 Introduction

1.1 Identifying information

Architecture Name: **smartrail 4.0 Overall System Architecture**

System of Interest: **smartrail 4.0**

1.2 Purpose

This document provides an overview of the smartrail 4.0 Overall System Architecture. The architecture is described using multiple views.

1.3 Scope

As the smartrail 4.0 Overall System is composed of subsystems of substantial size, this document is focusing on the overarching concepts. The details of each subsystem will be documented in its own documents. The subsystems defined in this architecture are building blocks, that can be used either all or only some of them by the WI-7179 - Infrastructure Manager, depending on its need.

1.4 System Overview

A system overview including the system scope and system boundary is described in System Definition Document Deutsch.

2 Architectural Goals and Constraints

2.1 Non-Functional Requirements

The non-functional requirements are one of the main driver for the architecture. They are collected in the document Nichtfunktionale Anforderungen.

2.2 Criteria for Decomposition

Basically, a required functionality can be distributed in countless variants to subsystems (hardware and software). However, since this distribution has a huge effect on properties like life-cycle costs (LCC) or quality attributes (QA), the optimal distribution must be chosen with regard to these properties. In order to achieve this, the following criteria are defined for dividing the systems into subsystems:

- Thin Safety-Layer
- Separate high available function from less available functions
- Separate along expected expected Life-Cycle, due to:
  - Independent change rate or independent impact of changes
  - Independent release also due to expected technology changes or risk mitigation
  - Independent life duration
- Separate when used by different WI-7179 - Infrastructure Manager
- Narrow and well testable interface (low coupling) and high functional cohesion
- Strategy for product like: off the shelf products, make or buy, IT Strategy, procurement strategy
- Required hardware borders (e.g. geographically distributed, independently movable)
- Separate when different or multiple suppliers
- Assessment strategy (e.g. how easy is the assessment)

3 Views

3.1 System Structure View

This view shows how the overall system is built up from logical blocks, where each block is a principal unit of processing logic or control entity. The blocks are interconnected by communication interfaces. Some of the blocks are pure software and some of the blocks are hardware and software combined. The blocks have independent life cycles, which means they should be developed, tested, released, assessed, accepted and operated independently of each other. It is possible that some of the blocks themselves consist of multiple smaller blocks that have independent life cycles.

3.1.1 Primary Presentation
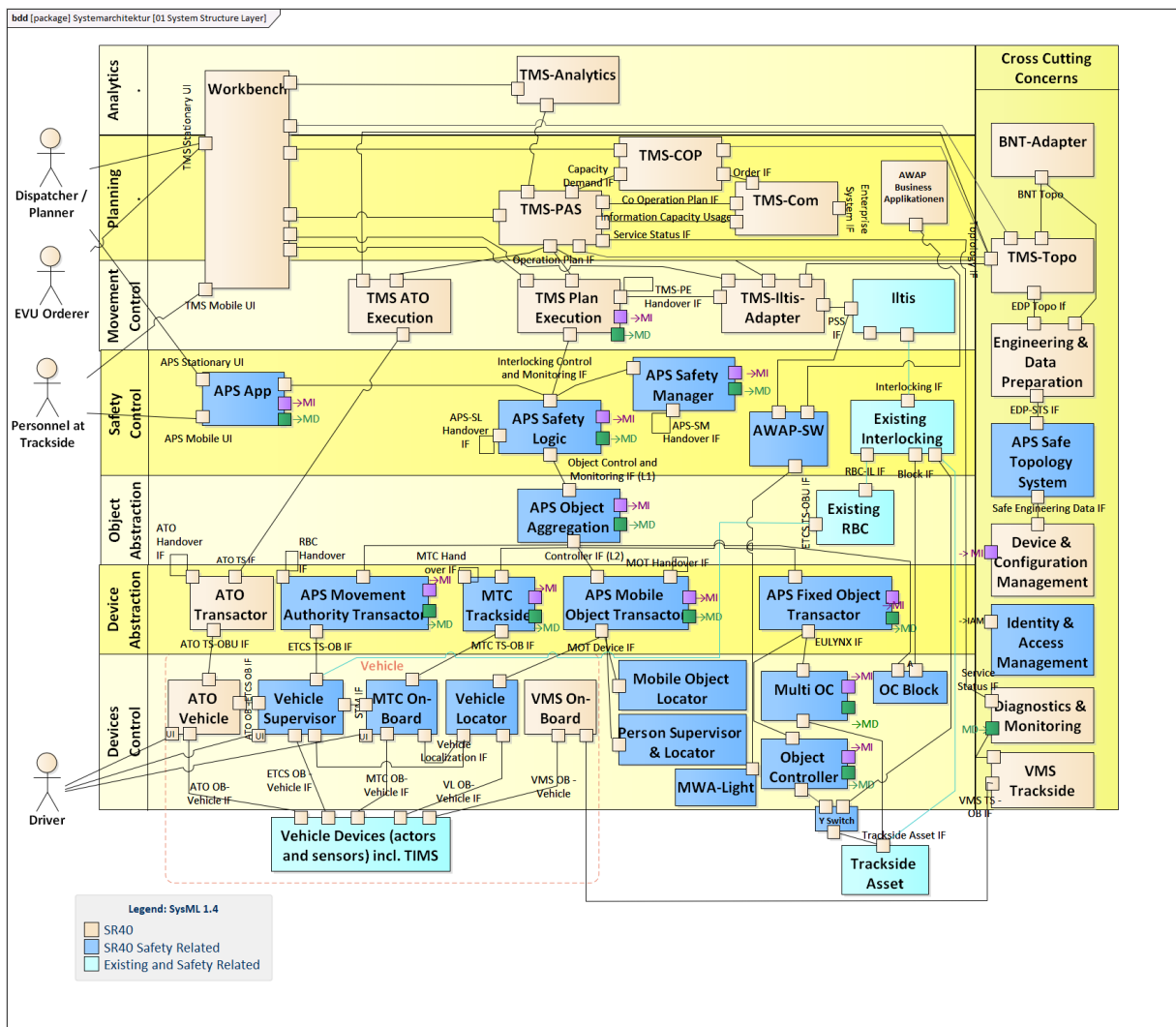
Summary of the most important points (details see in the Element Catalog below):

- The SRP-3087 - TMS-PAS creates and optimizes the WI-2247 - Capacity Plan (schedules) over all time horizons. This will also result in a WI-2248 - Operation Plan (German: WI-1051 - Produktionsvorgabe) that contains a conflict-free and detailed specification of the capacity usage (track occupancy) for the next few hours. The SRP-3086 - TMS Plan Execution, the SRP-3085 - TMS ATO Execution, the SRP-3088 - TMS-Iltis-Adapter and their underlying systems execute the WI-2248 - Operation Plan and provide back to SRP-3087 - TMS-PAS the WI-3263 - ExecutionState of the WI-2248 - Operation Plan. The WI-2248 - Operation

Plan interface is the same interface for the different ways to implement the 📦WI-2248 - Operation Plan like 📦 SRP-3086 - TMS Plan Execution or 📦SRP-3088 - TMS-Iltis-Adapter.

- The 📦SRP-3068 - APS Object Aggregation combines the information from the outside world (e.g. train position information and trackside TDS state) received from the underlying blocks to one consolidated representation that is provided to the 📦SRP-3066 - APS Safety Logic. In the other communication direction, it dispatches information from the 📦SRP-3066 - APS Safety Logic to the outside world using the underlying blocks.

- The safety related blocks (blue in the diagram) shall contain as little non-safety related functionality as possible, according to a initial assessment, that needs to be justified later.. As a consequence 📦SRP-3086 - TMS Plan Execution has to send detailed requests to 📦SRP-3066 - APS Safety Logic. In addition the ATO functionality is implemented without safety responsibility in 📦SRP-3083 - ATO Transactor, 📦SRP-3084 - ATO Vehicle and 📦SRP-3085 - TMS ATO Execution separated from the safety-related blocks.

- To achieve latency performance and availability, 📦SRP-3086 - TMS Plan Execution, 📦SRP-3088 - TMS-Iltis-Adapter and their underlying systems can run per geographical region and not once for the entire transport network. This increases the availability, because in most cases the impact of a software faults, a security vulnerability or wrong manipulation is limited to one region. To achive this for software faults the following measures shall be implemented: The software is for a first period of time only deployed to one region and after success, deployed stepwise to the other regions.

3.1.2 Element Catalog

3.1.2.1 Blocks

SRP-3087 - TMS-PAS

The **TMS-PAS** (**P**roduktions-**A**utomatisierungs**s**ystem) creates and optimizes the 📦WI-2247 - Capacity Plan over all time horizons based on multiple service intentions. The schedule contains all aspects of track usage including 📦 WI-2400 - Train Run, 📦WI-2402 - Shunting Movement, 📦WI-2403 - Stabling, maintenance work, construction work and inspection. TMS-PAS

generates from 📦WI-2247 - Capacity Plan an 📦WI-2248 - Operation Plan (Produktionsvorgabe) that specifies the exact track usage including the sequence of usage for the execution of the plan. **TMS-PAS** also optimizes the schedule of the current day according to the current 📦WI-3263 - ExecutionState and calculates near real-time schedule adjustments to avoid conflicts. In case of a disruption, **TMS-PAS** is responsible for the immediate rescheduling all affected track usages. [🌵approved]

SRP-3089 - TMS-Com

TMS-Com is the central entity for exchanging information between the blocks of TMS and the external data consumers and data producers. It aggregates and prepares the data for the external data consumers and data producers such that only one consolidated interface per topic is used within TMS. **TMS-Com** acts as an abstraction layer for different external systems and data structures. [🌵approved]

SRP-3090 - TMS-Analytics

The **TMS-Analytics** allows analyzing performance and regulatory risk reporting from the collected data. It provides reports for valuating and further developing the system in relation to segments, products, customers, contact points or competitors, as well as for providing market analysis and research. [🌵approved]

SRP-3092 - TMS-Topo

The **TMS-Topo** provides the topological data for different time horizons to the different TMS blocks, where the topological data is generated out of existing topological data. In addition, it manages data for future infrastructure changes as abstract "resource models", such that the long-term capacity planning is possible. [approved]

SRP-13189 - BNT-Adapter

The **BNT-Adapter** transforms the topology from the legacy data format to the new standard BNT format. The BNT is the common data model that was decided to be used in smartrail 4.0. The topology data is provided to the SRP-3092 - TMS-Topo as well as to SRP-9489 - Engineering & Data Preparation. As the different WI-7179 - Infrastructure Manager may have other sources for the topology data, there may be different implementations of the **BNT-Adapter** for the different WI-7179 - Infrastructure Manager. [approved]

SRP-3093 - Workbench

The **Workbench** implements the connection with customer and employee interaction. These include services relating to sell, plan, settle up and manage all the different TMS aspects of different channel possibilities like stationary or mobile. The mobile variant provides the user interface to the WI-2327 - Personnel at Trackside and the WI-2831 - Engine Driver. This allows to request WI-2402 - Shunting Movement, to request access to the tracks or to control the SRP-5014 - Trackside Assets by interacting directly with the system. [approved]

SRP-4641 - TMS-COP

The **TMS-COP** (**C**apacity-**O**rdering-**P**ortal) provides the functionality related to the ordering and selling of capacity, which includes the tracking of the entire workflow. It will provide the requested capacity to SRP-3087 - TMS-PAS and it will receive from SRP-3087 - TMS-PAS the WI-2247 - Capacity Plan.

 [approved]

SRP-3085 - TMS ATO Execution

The **TMS ATO Execution** generates from the WI-2248 - Operation Plan the required information for the standardized interface SRP-4935 - ATO TS Interface to the SRP-3083 - ATO Transactor. [approved]

SRP-3083 - ATO Transactor

The **ATO Transactor** implements the communication with the SRP-3084 - ATO Vehicle and provides the standardized interface SRP-4935 - ATO TS Interface. The collaboration with a neighboring ATO Transactor is done over the SRP-4932 - ATO Handover Interface. It can be easily used by other WI-7179 - Infrastructure Managers, because it uses standardized interfaces. [approved]

SRP-3084 - ATO Vehicle

The **ATO Vehicle** operates the vehicle automatically and optimizes the speed such that it reaches given points at the given times as received over the SRP-4880 - ATO TS - OB Interface. It also communicates with the SRP-3081 - Vehicle Supervisor over the SRP-4925 - ATO OB - ETCS OB Interface. [approved]

SRP-3086 - TMS Plan Execution

The **TMS Plan Execution** generates the requests to the SRP-3066 - APS Safety Logic at the right point in time to execute the WI-2248 - Operation Plan. According to the progress it reports the WI-3263 - ExecutionState of the WI-2248 - Operation Plan back to SRP-3087 - TMS-PAS. The WI-3263 - ExecutionState describes the parts of the plan that are already executed and the parts of the plan that are already allocated (e.g. when WI-1974 - Movement Permission is already set).

TMS Plan Execution shall easily be rolled out and operated with the SRP-3066 - APS Safety Logic independent of SRP-3087 - TMS-PAS such that the SRP-3066 - APS Safety Logic can also be used by WI-7179 - Infrastructure Manager that do not use SRP-3087 - TMS-PAS. [approved]

SRP-3088 - TMS-Iltis-Adapter

The **TMS-Iltis-Adapter** converts the WI-2248 - Operation Plan into scheduling information for the existing system SRP-5015 - Iltis. The WI-3263 - ExecutionState of the WI-2248 - Operation Plan is extracted from the SRP-5015 - Iltis state information. When the scheduling information is edited in SRP-5015 - Iltis, the changed scheduling information is also included in the WI-3263 - ExecutionState. For other traffic control system, a similar application TMS-XYZ-Adapter has to be developed. [approved]

SRP-3066 - APS Safety Logic

The **APS Safety Logic** decides if a request is granted or rejected depending on the resulting risk. The request can ask for a state change of an SRP-5014 - Trackside Asset / Warning Area or the creation / modification / removal of a WI-1974 - Movement Permission or a WI-1996 - Usage Restriction Area. For the decision, the **APS Safety Logic** stores the state of the SRP-5014 - Trackside Assets, the WI-1974 - Movement Permissions, the position of the WI-2036 - Movable Objects (e.g. trains), the current WI-1996 - Usage Restriction Areas. and the topological data. A request shall only be granted if it does not cause a danger pattern of SRP-3069 - APS Safety Manager. [approved]

SRP-3069 - APS Safety Manager

The **APS Safety Manager** continuously monitors the state of the system, such that it can recognize patterns that are identifying hazardous situations. It will trigger one or several reactions (e.g. emergency stop of a WI-2036 - Movable Object, reduction of the speed, extend WI-1974 - Movement Permission) to prevent or minimize the damage. In addition it also recognizes situations that require the warning of an WI-2036 - Movable Object (e.g WI-2327 - Personnel at Trackside). [approved]

SRP-3068 - APS Object Aggregation

The **APS Object Aggregation** combines the information received over different channels from the trackside world to one consolidated representation that is provided to the SRP-3066 - APS Safety Logic. That consolidated representation contains the state of the WI-2036 - Movable Object (e.g. trains) like position and extend as well as the state of the SRP-5014 - Trackside Assets. In the other communication direction, it dispatches information from the SRP-3066 - APS Safety Logic using the corresponding communication channels to the outside world. This information includes the WI-1974 - Movement Permissions, the state request for the SRP-5014 - Trackside Asset and warning messages for WI-2327 - Personnel at Trackside and WI-2831 - Engine Driver. [approved]

SRP-3080 - APS Movement Authority Transactor

The **APS Movement Authority Transactor** communicates with the registered ETCS capable vehicles. Among others it translates the WI-1974 - Movement Permissions to ETCS Movement Authorities and sends them to the vehicle. In the other direction it will receive the train position reports from the vehicle and forward them to the SRP-3068 - APS Object Aggregation. [approved]

SRP-3081 - Vehicle Supervisor

The **Vehicle Supervisor** displays to the "Driver" the current allowed Movement Authority by using cab signaling. It also supervises the speed and ensures that the train does not violate its movement authority. Further it will sent the current position as a "Train Position Report" to the SRP-3080 - APS Movement Authority Transactor. [approved]

SRP-9993 - MTC Trackside

The **MTC Trackside** communicates with the registered MTC capable vehicles. It provides the relevant information like the WI-1974 - Movement Permission to supervise the movement of the vehicle. In the other direction it provides information like the train position and train extend.
[approved]

SRP-9992 - MTC On-Board

The **MTC On-Board** implements additional functionality that is not available in the SRP-3081 - Vehicle

Supervisor due to its standardized ETCS interface. The MTC is mainly used for slow speed (e.g. Shunting) and as a redundant system. It displays to the "Driver" the current allowed WI-1974 - Movement Permission by using cab signaling. It also supervises the speed and ensures that the train does not violate its WI-1974 - Movement Permission. Further it will sent the current position and extend to the SRP-9993 - MTC Trackside. A Redundant Safety Layer (RSL) is part of MTC On-Board (to discuss if RSL is a component independent from MTC On-board) and is used in case of TMS or EI failure to ensure a minimal safety level. RSL prevents collision regarding only relative distances between trains.
[approved]

SRP-3071 - APS Fixed Object Transactor

The **APS Fixed Object Transactor** enables the connection of an SRP-3072 - Object Controller to the SRP-3068 - APS Object Aggregation. Therefore it translates between the generic SRP-4705 - Controller Interface to the more specific SRP-5008 - EULYNX Interface. [approved]

SRP-3072 - Object Controller

The Object Controller is an subsystem controlling and monitoring the trackside assets. It implements the standard interface defined by EULYNX. There is a separate specific OC-Types defined for each type of SRP-5014 - Trackside Asset (e.g. a point). [approved]

The following specific "OC" are used. They are just shown as "Object Controller" in the above diagram.

SRP-13287 - OC - Point

The OC - Point is the EULYNX subsystem - Point. It provides the standard interface SRP-13173 - EULYNX SCI-P - Point Interface for accessing the trackside asset.

SRP-13289 - OC - Level Crossing

The OC - Level Crossing is the EULYNX subsystem - Level Crossing [approved]

SRP-13288 - OC - Light Signal

The OC - Light Signal is the EULYNX subsystem - Light Signal [approved]

SRP-13290 - OC - Train Detection System

The OC - Train Detection System is the EULYNX subsystem - Train Detection System [approved]

SRP-13712 - Y Switch

Technical solution that provides, during the migration phase, a switching mechanism to alternate the control of Trackside Assets (TA) between old and new interlocking systems during migration. [approved]

SRP-13719 - Multi OC

A system which represents more than one OC (OC in the EULYNX terminology) . Multi OCs are primary existing electronic interlocking systems that support the Multi OC Mode

SRP-3076 - OC - Block

The **OC - Block** implements the block interface to the SRP-5016 - Existing Interlocking, such that the WI-2036 - Movable Objects (e.g. trains) can pass over the border to and from the SRP-5016 - Existing Interlocking. [approved]

SRP-3070 - Object Controller Next

The **Object Controller Next (OCN)** monitors and controls one or multiple SRP-5014 - Trackside Assets. The Object Controller Next is either installed in the interlocking room or in the field directly at the SRP-5014 - Trackside Asset. It has no EULYNX interface, but is directly connected with SRP-3068 - APS Object Aggregation over the SRP-4705 - Controller Interface. This allows to implement functionality that is currently not foreseen with the EULYNX interface (example: doors in a tunnel). [approved]

Note: The ⬢SRP-3070 - Object Controller Next is not shown in the above diagram.

SRP-3073 - APS Mobile Object Transactor

The **APS Mobile Object Transactor** manages the different kinds of localisation devices and provides them the necessary information to localize themselves. The **APS Mobile Object Transactor** processes the received localization information such that it can be forwarded to the ⬢SRP-3068 - APS Object Aggregation. It also forwards warning information to the localisation devices. If necessary, the **APS Mobile Object Transactor** also processes localisation-related information that could not be provided over ▱SRP-4732 - ETCS TS - OB interface to the ⬢SRP-3077 - Vehicle Locator. **[➡🌵 approved]**

SRP-3077 - Vehicle Locator

The **Vehicle Locator** provides the ⬢SRP-3081 - Vehicle Supervisor with its current position. If necessary, it may in addition send localisation-related information that can't be sent over ▱SRP-4732 - ETCS TS - OB interface to ⬢ SRP-3073 - APS Mobile Object Transactor. **[🌵 approved]**

SRP-3074 - Person Supervisor & Locator

The **Person Supervisor & Locator** can be set up to warn or authorize the person or a group of persons when a moveable object / vehicle approaches. The warning is done in accordance to pre-configured warning areas. In addition it can locate itself and block the track where it is set up. It can be a trackworker safety system, a tag or an app on a tablet that interacts with the person. **[➡🌵 approved]**

SRP-3075 - Mobile Object Locator

The **Mobile Object Locator** sends its current location to the ⬢SRP-3073 - APS Mobile Object Transactor. It can be used for multiple use cases like tagging an obstacle, a crane, a train-end a wagon or coach, a door that swings on the track or ▦WI-2327 - Personnel at Trackside. **[➡🌵 approved]**

SRP-5013 - APS Safe Topology System

The **APS Safe Topology System** ensures correct topology and topography data for SIL4 applications by combining information from different sources, which also includes the acquisition of data by mobile measurement devices in the field. **[🌵 approved]**

SRP-9489 - Engineering & Data Preparation

The **Engineering & Data Preparation (EDP)** provides the configuration data for the safety-related subsystems and ⬢ SRP-3086 - TMS Plan Execution. It highly automates the process of planning, commissioning and homologation. **[🌵 approved]**

SRP-4643 - APS App

The APS App provides a stationary as well as a mobile user interface that is used to display safety related information (e.g. track is blocked with ▦WI-1996 - Usage Restriction Area for construction work) and to allow safety related input (e.g. track is free again from construction work such that ▦WI-1996 - Usage Restriction Area can be removed). All the user interaction that are not safety relevant are done using the ⬢SRP-3093 - Workbench that is running on the same device as the **APS App**. **[➡🌵 approved]**

SRP-4644 - Identity & Access Management

The **Identity & Access Management** authenticates and authorizes users and technical systems and grants or denies access to the system. Therefore it will need to store the credentials to authenticate the entities as well as the autorisation information for each identity. **[➡🌵 approved]**

SRP-9995 - Device & Configuration Management

The **Device & Configuration Management** is used to setup and manipulate the APS Components, ⬢SRP-9993 - MTC Trackside, ⬢SRP-3086 - TMS Plan Execution and components deployed on ⬢SRP-4962 - CCS onboard application platform for trackside related functions (COAT). This includes updating the configuration data and the software

version. **[** approved **]**

SRP-9994 - Diagnostics & Monitoring

The **Diagnostics & Monitoring** collects monitoring and diagnostics information from all the capacity relevant infrastructure like SRP-5014 - Trackside Asset and the vehicles. The information is on one side used to derive the capacity limitation and an estimated duration of the capacity limitation that is used to reschedule the WI-2247 - Capacity Plan . On the other side the information is forwarded to a monitoring system of the company that triggers the corrective maintenance actions. **[** approved **]**

SRP-9997 - VMS On-Board

The **VMS** (**V**ehicle **M**onitoring **S**ystem) **On-Board** collects the capacity relevant information of the vehicle that is used to optimize the capacity plan. **[** approved **]**

SRP-9996 - VMS Trackside

The **VMS** (**V**ehicle **M**onitoring **S**ystem) **Trackside** communicates with the registered vehicles that are capable of providing monitoring information. It forwards the monitoring state to the SRP-9994 - Diagnostics & Monitoring. **[** approved **]**

SRP-4642 - AWAP Business Applikationen

The **AWAP Business Applikationen** allows the user to plan and define warning areas that are later used for the SRP-17915 - AWAP-SW to warn at the right point in time.
[approved **]**

SRP-17915 - AWAP-SW

The **AWAP-SW** is the central component that generates the warn information for the SRP-22515 - MWA Light when SRP-5015 - Iltis is used. **[** approved **]**

SRP-22515 - MWA Light

The **MWA Light** is the system at trackside, which warns the WI-2327 - Personnel at Trackside when a train is approaching. This is used together with the SRP-17915 - AWAP-SW.
[approved **]**

3.1.2.2 External Blocks

SRP-5014 - Trackside Asset

The **Trackside Asset** is the hardware (in some cases including embedded software) that needs to be monitored and controlled such that the WI-2036 - Movable Object (e.g. trains) can run safely on the tracks. **[** approved **]**

SRP-5016 - Existing Interlocking

The **Existing Interlocking** are interlocking systems that are controlling the trains safely today. This includes relay interlocking and computer based interlocking. The interlocking can be remotely monitored and controlled by the following means

- computer based interlocking: Includes an electronic interface
- relay interlocking: Needs an IO-Device (e.g. rcs95), that provides the electronic interface

[approved **]**

SRP-9998 - Existing RBC

The **Existing RBC** is the RBC that is used today for an ETCS Level 2 area to control and monitor the vehicle. Among others it transmit the routes from the SRP-5016 - Existing Interlocking to the vehicle and receives the current position from the vehicle **[** approved **]**

SRP-5015 - Iltis

The **Iltis** is the currently installed traffic control system. It includes the functionality to remotely monitor and control the interlocking in a manual way. It also includes automation functions like the train describer or the automatic route setting.
[approved]

SRP-5017 - Vehicle Devices (actors and sensors) incl. TIMS

The **Vehicle Devices** represents the devices (sensors and actors) on the vehicle (such as engine, brakes, …) that allows to brake, to cut off the traction and to accelerate the vehicle. It is not part of the smartrail 4.0 system. [approved]

3.1.2.3 Interfaces

SRP-4655 - Operation Plan Interface

The **Operation Plan Interface** provides the WI-2248 - Operation Plan from the planning part to the control part and gives the current execution state back to the planning level. It includes the following information:
Downstream:

- The current version of the WI-2248 - Operation Plan includes:
    - In the case of a WI-2260 - Capacity Object (WI-2400 - Train Run, WI-2402 - Shunting Movement, WI-2403 - Stabling):
        - The track-precise path defined for the WI-2260 - Capacity Object
        - The order in which the different WI-2260 - Capacity Object are allowed to use each track
        - Time constraints for departure, arrival or pass-through at certain points in the track network.
        - Relations between WI-2260 - Capacity Object for interconnections, usage of vehicles and personnel.
        - The optimized speed profile.
    - In the case of a planned WI-2261 - Capacity Restriction (e.g. planned maintenance work)
        - The affected area on the topology
        - The start and end time of the limitation.
        - Details about the limitation like allowed speed.
        - The order relative to the track usage of the WI-2260 - Capacity Object, such that a WI-2261 - Capacity Restriction is not activated before the preceding WI-2260 - Capacity Object have used the track.

Upstream:

- The execution status for each WI-2260 - Capacity Object/ WI-2261 - Capacity Restriction. The status is not only provided for the objects planned in the WI-2248 - Operation Plan but also for unplanned objects (e.g. unavailable track due to an failure).

SRP-5044 - TMS-PE Handover Interface

The **TMS-PE Handover** Interface is used between two SRP-3086 - TMS Plan Execution or a SRP-3086 - TMS Plan Execution and a SRP-3088 - TMS-Iltis-Adapter to pass a WI-2036 - Movable Object from one region to the next.

SRP-4729 - Interlocking Control and Monitoring Interface

The **Interlocking Control and Monitoring Interface** allows that the non-safety related block requests state changes from the interlocking logic and monitors the interlocking logic. It includes the following main information:
Downstream:

- Request state change of a WI-6947 - Drive Protection Section
- Request WI-1974 - Movement Permission for a WI-2036 - Movable Object (e.g. train)
- Request changes for WI-1996 - Usage Restriction Area
- Request Warning

Upstream:

- Provides the current state of a WI-6947 - Drive Protection Section (e.g. SRP-5014 - Trackside Asset).
- Provides the state of the WI-2036 - Movable Objects (e.g. trains).position and the extent
- Provide WI-1996 - Usage Restriction Area
- Provide the activation of the topology of the track network

  This information is used, when the topology changes, such that the consumer of this interface knows the current active topology.

SRP-5045 - APS-SL Handover Interface

The **APS-SL Handover Interface** is used to pass a WI-2036 - Movable Object from one SRP-3066 - APS Safety Logic to the next. The vehicle needs to receive WI-1974 - Movement Permissions in such a way, that it can drive from one SRP-3066 - APS Safety Logic to the next without stopping. The two instance can be from two different WI-7179 - Infrastructure Manager or the same.

SRP-19861 - APS-SM Handover Interface

The **APS-SM Handover** Interface is used to coordinate the work between different instances of the SRP-3069 - APS Safety Manager for recognize danger pattern and for executing the corresponding safety-reaction.

SRP-4628 - Object Control and Monitoring Interface

The **Object Control and Monitoring** interface is a business logic oriented high level interface between an interlocking logic and the outside world that it controls. It includes the following information:

Downstream:

- Requests a state change of a WI-6947 - Drive Protection Section
- Grant WI-1974 - Movement Permissions to the WI-2036 - Movable Objects (e.g. trains)
- Warn WI-2036 - Movable Objects (e.g. WI-2327 - Personnel at Trackside)
- The Activation of a Topology of the track network.

Upstream:

- Provides the current state of a WI-6947 - Drive Protection Section
- Provides the position and the extend of all the WI-2036 - Movable Objects (e.g. trains).

SRP-4705 - Controller Interface

The Controller Interface is an single controller oriented interface. A single control can provide or consume only part of the control or monitor information. It includes the following information:

Downstream:

- Requests a state change of a WI-6947 - Drive Protection Section
- Grant WI-1974 - Movement Permissions directly to the WI-2036 - Movable Objects (e.g. trains) or indirectly via a trackside signal.
- Warn a WI-2036 - Movable Objects (e.g. WI-2327 - Personnel at Trackside)
- The Activation of a Topology of the track network.

Upstream:

- Provides the current state of a WI-6947 - Drive Protection Section
- Provides information about the position and extend of a WI-2036 - Movable Object. The information can already be assigned to a WI-2036 - Movable Object or be just location based without an assignment to a WI-2036 - Movable Object (e.g. occupancy of an track).

SRP-5018 - MOT Device Interface

The **MOT Device Interface** is used to communicate between the SRP-3073 - APS Mobile Object Transactor and the connected devices, which includes SRP-3077 - Vehicle Locator, SRP-3074 - Person Supervisor & Locator and SRP-3075 - Mobile Object Locator. It includes the following information:

- Management of the devices
- Information of the physical objects that is being represented by a device
- Provides information to the device, which it needs to localize itself.
- Position of the device
- Requests to warn the WI-2036 - Movable Object or WI-2327 - Personnel at Trackside

SRP-12006 - MOT Handover Interface

The **MOT Handover Interface** is used to pass a device from one SRP-3073 - APS Mobile Object Transactor to the next.

SRP-12293 - VL OB - Vehicle Interface

The **VL OB - Vehicle Interface** provides the sensor information for the localization done in the SRP-3077 - Vehicle Locator .

SRP-4732 - ETCS TS - OB interface

The **ETCS TS (Trackside) - OB (On-Board) interface** is the ERTMS interface between trackside and vehicle equipment. It is specified in the following documents:

- SRP-4750 - ERTMS SUBSET-037 EuroRadio FIS
- SRP-4751 - ERTMS SUBSET-026 System Requirements Specification

Because there will still be vehicles based on baseline (BL) 2, the trackside must use on the interface System Version (SV) X=1. As a consequence the BL2 vehicle communicate with SV 1.0 and the BL3 vehicle communicate with SV 1.1. The trackside needs also to support the activation of SV 2.0 as soon as there are no more BL 2 vehicle running within the system boundaries.

SRP-4874 - ETCS OB - Vehicle Interface

The **ETCS OB Vehicle Interface** is the ERTMS interface for controlling the vehicle. It is specified in the following document:

- SRP-4875 - ERTMS SUBSET-034 Train Interface FIS

This Interface includes the following:

- Mode Control (Sleeping, Passive shunting, Non-Leading, Isolation)
- Control of Brakes (Service brake command, Brake pressure, Emergency brake command)
- Control of Train Functions (Traction Cut Off)
- Train Status (Cab Status, Direction Controller, Traction status)

- Train Data
- National System isolation

SRP-5046 - RBC Handover Interface

The **RBC Handover Interface** is the ERTMS interface to handle over a vehicle from one RBC to the next RBC. It is specified in the following documents:

- ⬌ SRP-5047 - ERTMS SUBSET-039 FIS for the RBC/RBC Handover
- ⬌ SRP-5048 - ERTMS SUBSET-098 RBC-RBC Safe Communication Interface

SRP-12323 - Vehicle Localization Interface

The Vehicle Localization Interface is the interface over which the 🔷 SRP-3077 - Vehicle Locator provides the current location of the vehicle to the other components on the vehicle.

SRP-4935 - ATO TS Interface

The **ATO TS (Trackside) interface** is between the ATO-TS and the planning system.

ATO over ETCS specifies this interface in the following document:

- ⬌ SRP-4939 - ATO over ETCS SUBSET-131 ATO-TS / TMS Interface Specification

SRP-4880 - ATO TS - OB Interface

The **ATO TS (Trackside) - OB (On-Board) interface** is between 🔷 SRP-3083 - ATO Transactor and vehicle equipment.

ATO over ETCS specifies this interface in the following document:

- ⬌ SRP-4882 - ATO over ETCS SUBSET-126 ATO-OB / ATO-TS Interface Specification

SRP-4923 - ATO OB - Vehicle Interface

The **ATO OB (On-Board) - Vehicle Interface** allows the ATO OB to control the vehicle.

ATO over ETCS specifies this interface in the following document:

- ⬌ SRP-4924 - ATO over ETCS SUBSET-139 ATO-OB / Vehicle Interface Specification

SRP-4925 - ATO OB - ETCS OB Interface

The **ATO OB - ETCS OB** Interface is used between the 🔷 SRP-3081 - Vehicle Supervisor and the 🔷 SRP-3084 - ATO Vehicle.

ATO over ETCS specifies this interface in the following document:

- ⬌ SRP-4926 - ATO over ETCS SUBSET-130 ATO-OB / ETCS OB Interface Specification

This Interface includes:

- ATO OB to ETCS OB
  - ATO Status ("AD Mode request", "ATO Engaged")
- ETCS OB to ATO OB
  - ETCS Train Data (e.g. "Train length", "Maximum Train Speed", "operational train running number")
  - Dynamic ETCS Data (e.g. "EB is requested", "Positioning Information", "MA Information", "Speed Information")

SRP-4932 - ATO Handover Interface

The **ATO Handover interface** is used to handover a vehicle from one 🔷 SRP-3083 - ATO Transactor to another 🔷

SRP-3083 - ATO Transactor.

ATO over ETCS specifies this interface in the following document:

- SRP-4933 - ATO over ETCS SUBSET-132 ATO-TS / ATO-TS Interface Specification

SRP-10361 - MTC TS - OB Interface

The MTC interface between SRP-9992 - MTC On-Board and SRP-9993 - MTC Trackside allows to control and monitor the vehicle in regards to the MTC functionality.

SRP-12073 - MTC OB Vehicle Interface

The MTC OB Vehicle interface is an interface for controlling the vehicle.

Compared to the ETCS OB Vehicle Interface it includes the following reduced set of functions:

- Mode Control (MTC Non-Leading, MTC Full Supervision, MTC Trip, MTC System Failure, MTC RSL)
- Control of Brakes (Service brake command, Brake pressure, Emergency brake command)
- Control of Train Functions (Traction Cut Off)
- Train Status (Cab Status, Direction Controller, Traction status)
- Train Data (reduced to a minimal set of standardized profiles)

SRP-12297 - MTC Handover Interface

The MTC Handover Interface is used to handover a vehicle from one SRP-9993 - MTC Trackside to another SRP-9993 - MTC Trackside.

SRP-12075 - STM Interface

The Specific Transmission Module (STM) Interface is an interface to switch between control by SRP-3080 - APS Movement Authority Transactor or SRP-9993 - MTC Trackside in order to ensure only one activated RTSA.

SRP-5223 - Trackside Asset Interface

The **Trackside Asset Interface** is the low level interface to control and monitor the SRP-5014 - Trackside Asset, which includes the switching of electric motors or lamps. There are many different variations of that interface.

SRP-5049 - Block Interface

The **Block Interface** is used at the system border to enter and leave WI-2036 - Movable Objects. This interface is used today between two SRP-5016 - Existing Interlockings to safely pass a train from one interlocking to the next.

SRP-5008 - EULYNX Interface

The **EULYNX interface** are the collection of interfaces defined by the EULYNX consortium for monitoring and controling the SRP-5014 - Trackside Asset. This includes:

- SRP-13173 - EULYNX SCI-P - Point Interface
- SRP-13292 - EULYNX SCI-LX - Level Crossing
- SRP-13293 - EULYNX SCI-TDS - Train Detection System
- SRP-13291 - EULYNX SCI-LS - Light Signal

SRP-13173 - EULYNX SCI-P - Point Interface

The SCI-P interface is the interface defined by the EULYNX consortium to control a point

SRP-13292 - EULYNX SCI-LX - Level Crossing

The SCI-LX interface is the interface defined by the EULYNX consortium to control a level crossing

SRP-13291 - EULYNX SCI-LS - Light Signal

The SCI-LS interface is the interface defined by the EULYNX consortium to control a light signal

SRP-13293 - EULYNX SCI-TDS - Train Detection System

The SCI-TDS interface is the interface defined by the EULYNX consortium to control a train detection system

SRP-13191 - BNT Topo Interface

The BNT Topo Interface is the standard interface to exchange topology data.

SRP-12322 - Topology Interface

The **Topology Interface** provides the current and future topology data including all the details needed for optimizng the capacity plan, that includes the details for checking the compatibility of a vehicle to the path in the topology as well as computing the travel time (e.g. maximum speed profile per "Cant Deficiency Train Category").

SRP-12324 - Engineering & Data Preparation - Topo Interface

The **Engineering & Data Preparation** - **Topo Interface** provides the CCS related configuration and topology data to be used by other systems.

SRP-10961 - Engineering & Data Preparation - Safe Topology System Interface

The **Engineering & Data Preparation - Safe Topology System Interface** is used to provide the data and the acquisition requests from SRP-9489 - Engineering & Data Preparation to SRP-5013 - APS Safe Topology System and to return the acquisition result in the opposite direction.

SRP-12325 - Safe Engineering Data Interface

The **Safe Engineering Data Interface** provides the "safe" WI-6949 - Engineering Data from the SRP-5013 - APS Safe Topology System to the SRP-9995 - Device & Configuration Management.

SRP-12326 - Identity & Access Management Interface

The Identity & Access Management Interface (IAM IF) provides services to authenticate and authorize human users and technical systems.

SRP-10102 - Capacity Demand Interface

The **Capacity Demand Interface** is used between SRP-4641 - TMS-COP and SRP-3087 - TMS-PAS for providing the demanded capacity derived from the orders.

SRP-12327 - Information Capacity Usage Interface

The **Information Capacity Usage Interface** provides detailed information for a capacity order, like the composition of the train.

SRP-12292 - Order Interface

The **Order Interface** is used between SRP-4641 - TMS-COP and SRP-3089 - TMS-Com for accepting the orders over a technical interface.

SRP-10565 - Co-Operation Plan Interface

The **Co-Operation Plan Interface** provide the relevant subset of the WI-2247 - Capacity Plan to the systems of the Railway Undertaker and the customer information system.

SRP-12339 - Analytics Data Provider Interface

The **Analytics Data Provider Interface** is used to collect all the data, that is used for the analytics.

SRP-10124 - PSS

The **PSS** is the central interface to Iltis.

SRP-10329 - Device Management Interface

The **Device Management Interface** is used between SRP-9995 - Device & Configuration Management and the managed blocks.

SRP-10898 - Diagnostics Interface

The **Diagnostics Interface** is used between ⬛SRP-9994 - Diagnostics & Monitoring and the monitored blocks.

SRP-10448 - VMS TS - OB Interface

The Vehicle Monitoring System Interface between On-Board and trackside allows to transmit the current state of the vehicle.

SRP-10449 - VMS OB - Vehicle Interface

The Vehicle Monitoring System Interface to the vehicle allows to acquire on-board the current state of the vehicle.

SRP-12328 - Service Status Interface

The **Service Status Interface** provides the information about the availability of an service. The status of the service is aggregated out of the status of all required subsystems.

SRP-12331 - TMS Plan Execution Workbench Interface

The **TMS Plan Execution Workbench Interface** is used to provide the information for the User Interface to ⬛ SRP-3093 - Workbench.

SRP-12330 - TMS-PAS Workbench Interface

The **TMS-PAS Workbench Interface** is used to provide the information for the User Interface to ⬛SRP-3093 - Workbench.

SRP-12333 - TMS-COP Workbench Interface

The **TMS-COP Workbench Interface** is used to provide the information for the User Interface from ⬛SRP-4641 - TMS-COP to ⬛SRP-3093 - Workbench.

SRP-12332 - TMS-Analytics Workbench Interface

The **TMS-Analytics Workbench Interface** is used to provide the information for the User Interface to ⬛SRP-3093 - Workbench.

SRP-12329 - TMS-Topo Workbench Interface

The **TMS-Topo Workbench Interface** is used to provide the information for the User Interface to ⬛SRP-3093 - Workbench.

3.1.3 User Interface

SRP-12336 - TMS Stationary UI

The **TMS Stationary UI** provides all the user interaction for the planners and dispatchers, who are located in the control centers and offices.

SRP-12335 - TMS Mobile UI

The **TMS Mobile UI** provides the user interaction for the ⬛WI-2327 - Personnel at Trackside including but not limited to entering a requests (e.g. request a ⬛WI-2402 - Shunting Movement) or display current information about next capacity usages.

SRP-12337 - APS Stationary UI

The **APS Stationary UI** provides the safety related display and control to the dispatcher.

SRP-12338 - APS Mobile UI

The **APS Mobile UI** provides the safety related display and control to the ⬛WI-2327 - Personnel at Trackside.

SRP-12340 - ETCS OB UI

The **ETCS OB UI** provides the user interaction with the ⬛WI-2831 - Engine Driver for the ETCS functionality.

SRP-12342 - MTC OB UI

The **MTC OB UI** provides the user interaction with the ⬛WI-2831 - Engine Driver for the MTC functionality.

SRP-12341 - ATO OB UI

The **ATO OB UI** provides the user interaction with the WI-2831 - Engine Driver for the ATO functionality.

3.1.4 Rationale

This chapter summarizes the rationale for the above described structure:

SRP-3096 - Separation according to the expected Safety-Relatedness

The functionality of the system is apportioned to the blocks such that the safety related functionality is separated from the non-safety related functionality as far as reasonable. As a consequence:

- The SRP-3066 - APS Safety Logic contains only the logic to decide if a request is permitted. The control sequence is implemented in SRP-3086 - TMS Plan Execution which is not safety related. For creating a WI-1974 - Movement Permission, SRP-3086 - TMS Plan Execution needs first to request the required state for a WI-6947 - Drive Protection Section. As soon as the required state is reached, it can issue the request for the WI-1974 - Movement Permission.
- The ATO functionality is implemented in SRP-3083 - ATO Transactor, SRP-3084 - ATO Vehicle and SRP-3085 - TMS ATO Execution separated from safety-related blocks.

SRP-3097 - Separation according to Availability and Latency Requirements

In order to achieve that not the whole system needs to comply to the same high availability and strict latency requirements, SRP-3086 - TMS Plan Execution receives from SRP-3087 - TMS-PAS the current WI-2248 - Operation Plan that contains all the detailed scheduling information. SRP-3086 - TMS Plan Execution implements the WI-2248 - Operation Plan with a short latency and a very high availability by sending a timely sequence of requests. SRP-3087 - TMS-PAS only needs to update the WI-2248 - Operation Plan when a significant deviation happens. The update can take more time, because until it is updated, the current WI-2248 - Operation Plan can still be used. As a consequence the SRP-3087 - TMS-PAS has lower availability and latency requirements.

SRP-12014 - Separation according to the usage by different Infrastructure Manager

In order to enable the usage of APS with an different planning system by other WI-7179 - Infrastructure Managers, SRP-3086 - TMS Plan Execution can be deployed together with EI and separated from SRP-3087 - TMS-PAS.

SRP-3098 - OC with independent Life-Cycle

The OC is separated from the rest of the system, such that it can have a independent life-cycle. This results in less costs because of the following:

- The OC can have a much longer lifespan. This will result in less investment costs, because there is a large number of OCs and each OC needs expensive hardware installation, including wiring.
- Single OCs that reaches its end-of-life can be replaced without the need to replace the other OCs in the same area.
- Extensions (e.g. a new point) can be realized by adding OCs without modifying the existing OCs.

SRP-3100 - Generic Controller Interface

The SRP-4705 - Controller Interface between SRP-3068 - APS Object Aggregation and the different transactors is defined in a generic way, containing only the relevant information for SRP-3068 - APS Object Aggregation in an abstract way. This enables to develop new type of controllers without changing the interface nor the SRP-3068 - APS Object Aggregation.

SRP-3101 - Separation of "APS Safety Logic", "APS Object Aggregation" und "EI SM"

The SRP-3066 - APS Safety Logic, SRP-3068 - APS Object Aggregation and SRP-3069 - APS Safety

Manager are separated according to the different expected change rate and different variability between the 📦WI-7179 - Infrastructure Manager.

Subsystem	Expected change rate	variability between the 📦WI-7179 - Infrastructure Manager
📦SRP-3066 - APS Safety Logic	low because the basic safety logic is stable.	Should be solved by parameters.
📦SRP-3068 - APS Object Aggregation	Medium change rate due to changes in sensors and actors	Different 📦WI-7179 - Infrastructure Manager may use a different mix of sensor and actors.
📦SRP-3069 - APS Safety Manager	Medium change rate to improvement resulting from feedback from the field.	Different patterns and reactions.

SRP-3212 - Separate TMS-Analytics

📦SRP-3090 - TMS-Analytics is separated from the rest of the system because there are different Quality Attributes required. In addition it allows to leverage specific technologies for analytics.

SRP-5059 - Separate TMS-COP

📦SRP-4641 - TMS-COP is separated from the rest of the system because there are different Quality Attributes required. In addition it allows to leverage specific technologies for building a portal for ordering and billing.
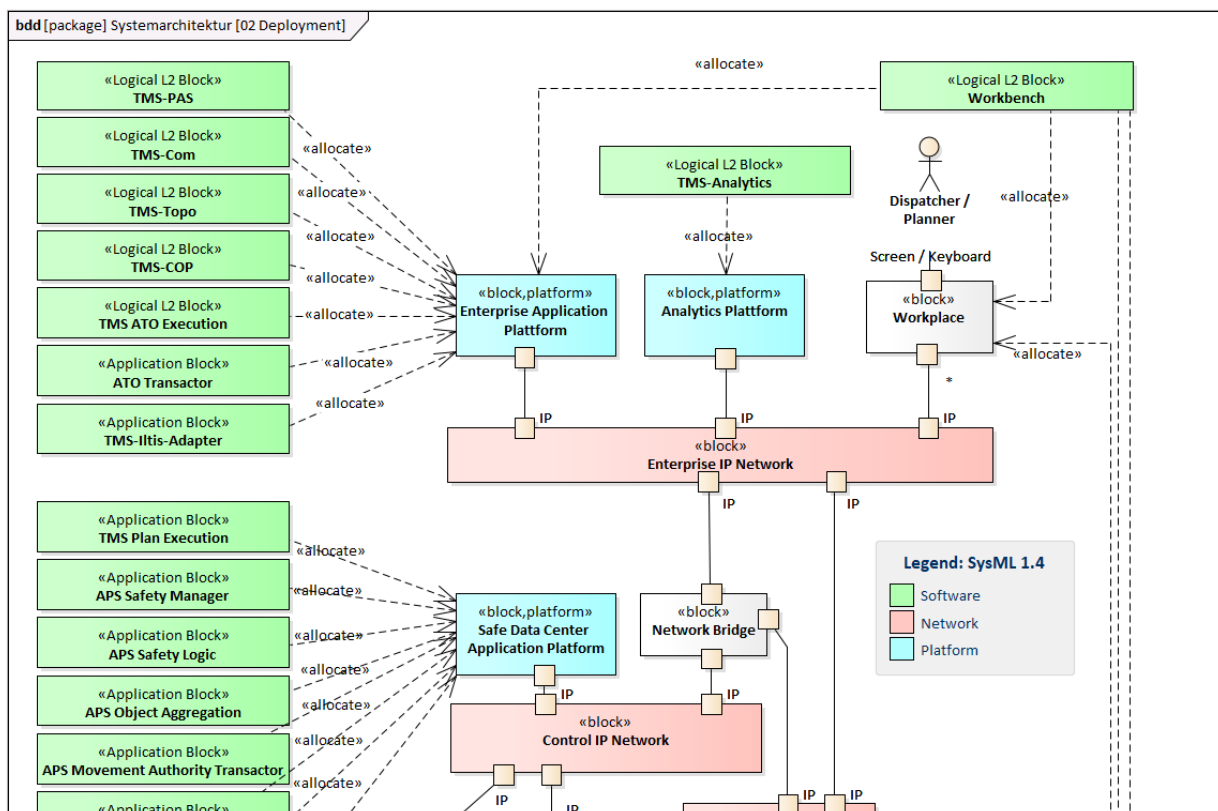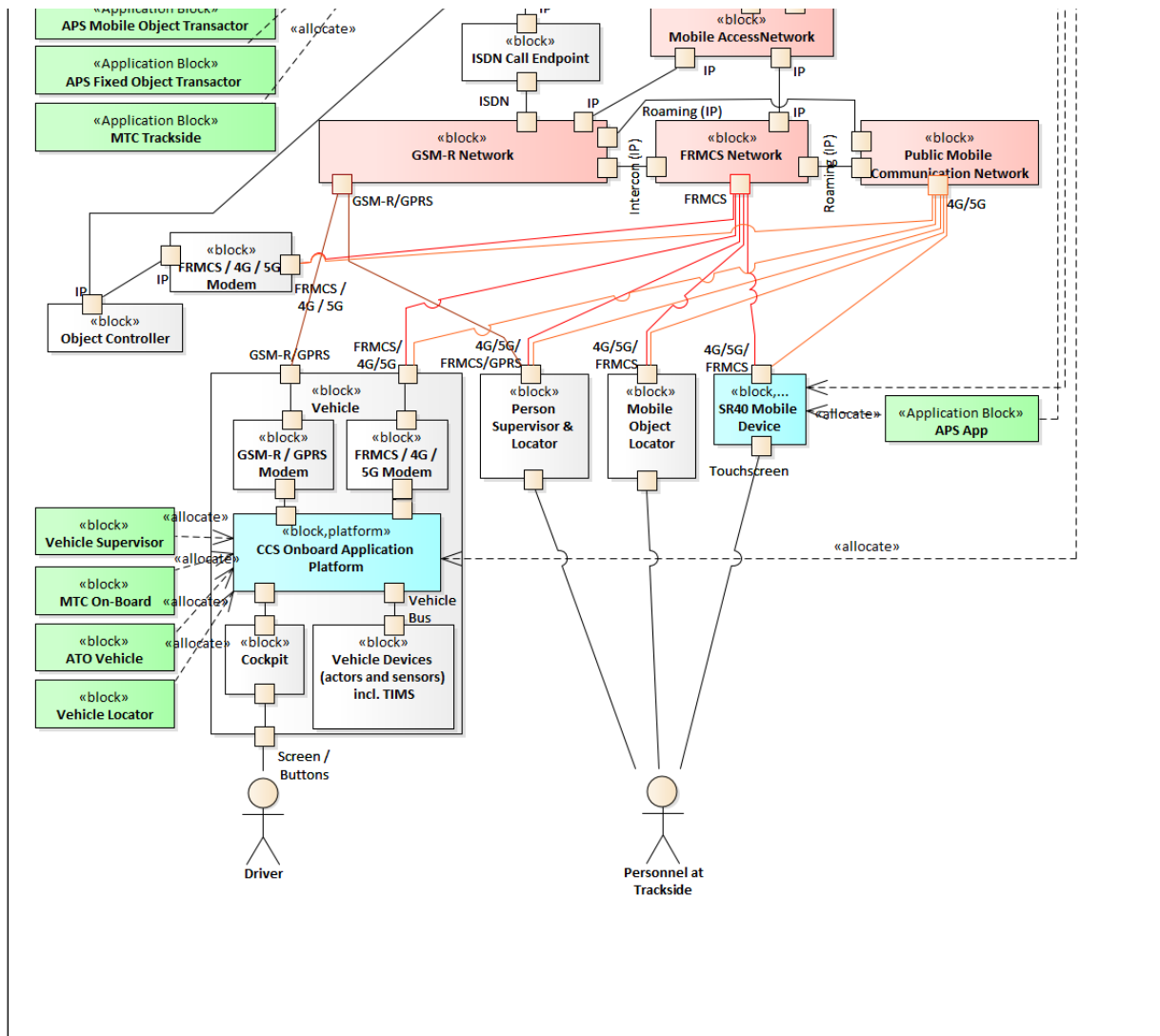
3.2 Deployment View

This view shows the hardware and communication network structure. In addition it also shows the allocation of Software to Hardware.

3.2.1 Primary Presentation

Summary of the most important points (details see in the Element Catalog below):

- The software is decoupled from the hardware and multiple software application can run on the same platform that consist of hardware and runtime environment. There are the following platforms: SRP-4950 - Enterprise Application Platform, SRP-4951 - Safe Data Center Application Platform, SRP-4961 - SR40 Mobile Device and SRP-4962 - CCS onboard application platform for trackside related functions (COAT).

- The mobile data network has an important role, because it connects not only the vehicles but also the SRP-4961 - SR40 Mobile Devices, the SRP-3075 - Mobile Object Locators and the SRP-3074 - Person Supervisor & Locator.

3.2.2 Element Catalog

3.2.2.1 Platforms

SRP-4950 - Enterprise Application Platform

The **Enterprise Application Platform** is the company platform to deploy business software.

For the concrete technologies used (e.g. for messaging) there are two set of technology stacks defined,

called "Enterprise" and "Realtime", where the "Realtime" is higher available and has shorter processing time. **[** approved **]**

SRP-11984 - Analytics Platform

The **Analytics Platform** is the company platform for data analytics. **[** approved **]**

SRP-4951 - Safe Data Center Application Platform

The **Safe Data Center Application Platform** provides an environment to run safety related software. It allows multiple

software to be developed, accepted and deployed independently of each other while sharing the same hardware. **[** approved **]**

SRP-4961 - SR40 Mobile Device

The **SR40 Mobile Device** is used by the WI-2327 - Personnel at Trackside and by the drivers on the vehicles. The SR40 Device allows to optimize the processes in the field. **[** approved **]**

SRP-4962 - CCS onboard application platform for trackside related functions (COAT)

The **CCS onboard application platform for trackside related functions** allows to have a standardized deployment target on the vehicle, which allows to use the same software on different vehicle types.

[approved **]**

3.2.2.2 Networks

SRP-4964 - GSM-R Network

The **GSM-R Network** is the already existing mobile network. Currently the vehicles communicate using the GSM-R

network by "calling" the RBC. This is a circuit switched (CS) data communication.

With ETCS BL 3.6 and higher the ETCS OBU and the RBC can also use (E)GPRS to communicate using packed switch

(PS) data communication. The use of (E)GPRS for ETCS is described in the following document: SRP-4979 - UIC

O-8664. As GSM-R will soon reach end-of-life, the GSM-R network won't be changed to use (E)GPRS. **[** approved **]**

SRP-4965 - FRMCS Network

The FRMCS (Future Railway Mobile Communication System) is the upcoming telecommunication technology defined

by UIC to replace GSM-R. The standard is not yet finalized. **[** approved **]**

SRP-4966 - Public Mobile Communication network

The Public Mobile Communication network is a 4G/5G mobile network from a public provider (e.g. Swisscom) that can

be used in Roaming. This will increase the availability. **[** approved **]**

SRP-4967 - Control IP Network

The Control IP Network connects the SRP-4951 - Safe Data Center Application Platform including the central running

software with the decentralized deployed SRP-3072 - Object Controller.

At SBB this is currently the "Datacom NG Rail Data" network. **[** approved **]**

SRP-4968 - Enterprise IP Network

The Enterprise IP Network is the basic communication network of the WI-7179 - Infrastructure Manager. It connects

all the different enterprise systems and workplaces of the company. **[** approved **]**

SRP-4978 - Mobile Access Network

The Mobile Access Network connects the SRP-4964 - GSM-R Network and the SRP-4965 - FRMCS Network via a bridge with the SRP-4967 - Control IP Network as well as with the SRP-4968 - Enterprise IP Network. [approved]

3.2.2.3 Other Subsystems

SRP-4985 - Network Bridge

The **Network Bridge** protects the SRP-4967 - Control IP Network from the SRP-4968 - Enterprise IP Network and the SRP-4978 - Mobile Access Network. It checks that only authenticated and authorized entities can send data into the SRP-4967 - Control IP Network. [approved]

SRP-4984 - ISDN Call Endpoint

The **ISDN Call Endpoint** accepts the GSM-R calls from the vehicle and forwards the data over the IP network to and from the SRP-3080 - APS Movement Authority Transactor which is running on the SRP-4951 - Safe Data Center Application Platform. This is needed for the first installations where GSM-R still need to be supportet. [approved]

SRP-4987 - Workplace

The **Workplace** is used by the stationary working actors to access the UI for interacting the system. This can be a standard PC or Laptop. [approved]

SRP-5057 - GSM-R / GPRS Modem

The **GSM-R / GPRS Modem** provides the connectivity to the SRP-4964 - GSM-R Network on the vehicle. This is needed for interoperability to ETCS installations that are still using GSM-R. [approved]

SRP-5058 - FRMCS / 4G / 5G Modem

The FRMCS / 4G / 5G Modem provides connectivity to the SRP-4965 - FRMCS Network and the SRP-4966 - Public Mobile Communication network on the vehicle. [approved]

3.2.3 Rationale

This chapter summarizes the rationale for the above described decomposition:

SRP-5060 - Separate Software from Hardware

The Software is separated from the hardware by having separate software applications running on standardized platforms. This allows independent life cycles of software applications and platforms. The hardware for example can be replaced without replacing the software application. Having separated platforms and multiple software applications allows to have multiple suppliers that reduces the vendor lock-in.

SRP-5061 - Multiple Software Application sharing the same Hardware

By running multiple software application on the same hardware, less hardware, less space and less energy is used.

SRP-22516 - Use different types of platforms

As there are different kind of software applications requiring different Quality Attributes, there is for each case the matching platform: SRP-4950 - Enterprise Application Platform, SRP-11984 - Analytics Platform, SRP-4951 - Safe Data Center Application Platform, SRP-4961 - SR40 Mobile Device and SRP-4962 - CCS onboard application platform for trackside related functions (COAT).

SRP-3099 - OC with Network Interface

The SRP-3072 - Object Controller can be controlled from a remote location over the network interface. This allows centralizing the rest of the safety-related functionality as software applications hosted on the SRP-4951 - Safe Data Center Application Platform.

SRP-4975 - Separate Control IP Network

The separate Control IP Network provides several benefits

- It is a measure of cyber security protection, because it reduces the exposure of the network. This corresponds to the Requirement **SR 5.1 – Network segmentation** of the ⬌ SRP-4976 - IEC 62443-3-3.
- It allows to increase the reliability, because it only contains the minimal infrastructure for its purpose. Where a network is also used for other purposes it will most probably consist of more devices such that it also can support other needs.
- It allows to have lower latency of the data communication, because there is no other data traffic that could yield to an overload of a node or link in the data network.
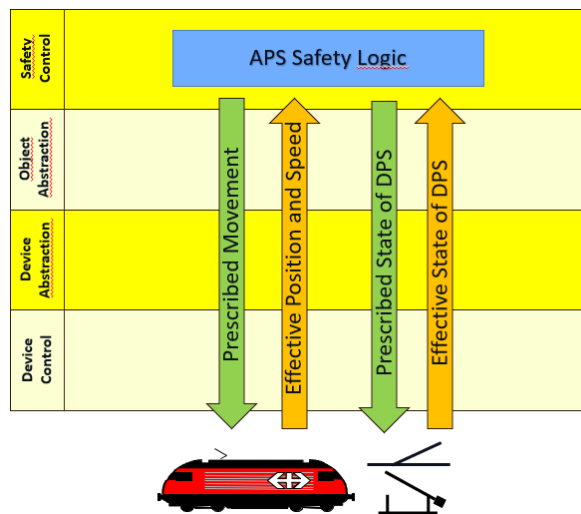
SRP-4977 - Separate Mobile Access Network

The ⬡ SRP-4964 - GSM-R Network and the ⬡ SRP-4965 - FRMCS Network will also handle data traffic from other systems that are running in the ⬡ SRP-4968 - Enterprise IP Network. Therefore the mobile data communication network cannot be connected directly to the ⬡ SRP-4967 - Control IP Network. But to increase the availability and to reduce the latency, the data traffic to the ⬡ SRP-4967 - Control IP Network shall not be routed over the ⬡ SRP-4968 - Enterprise IP Network. Therefore the ⬡ SRP-4978 - Mobile Access Network allows to connect the mobile data communication network to the bridge more directly.

3.3 (Safety-) Control Loops

This view shows the main Control Loops and how they are used to enforce a safe state of the overall system.

The main control for safety is that ⬡ SRP-3066 - APS Safety Logic prescribes a state for the "real world". The real world has to comply to the prescribed state.
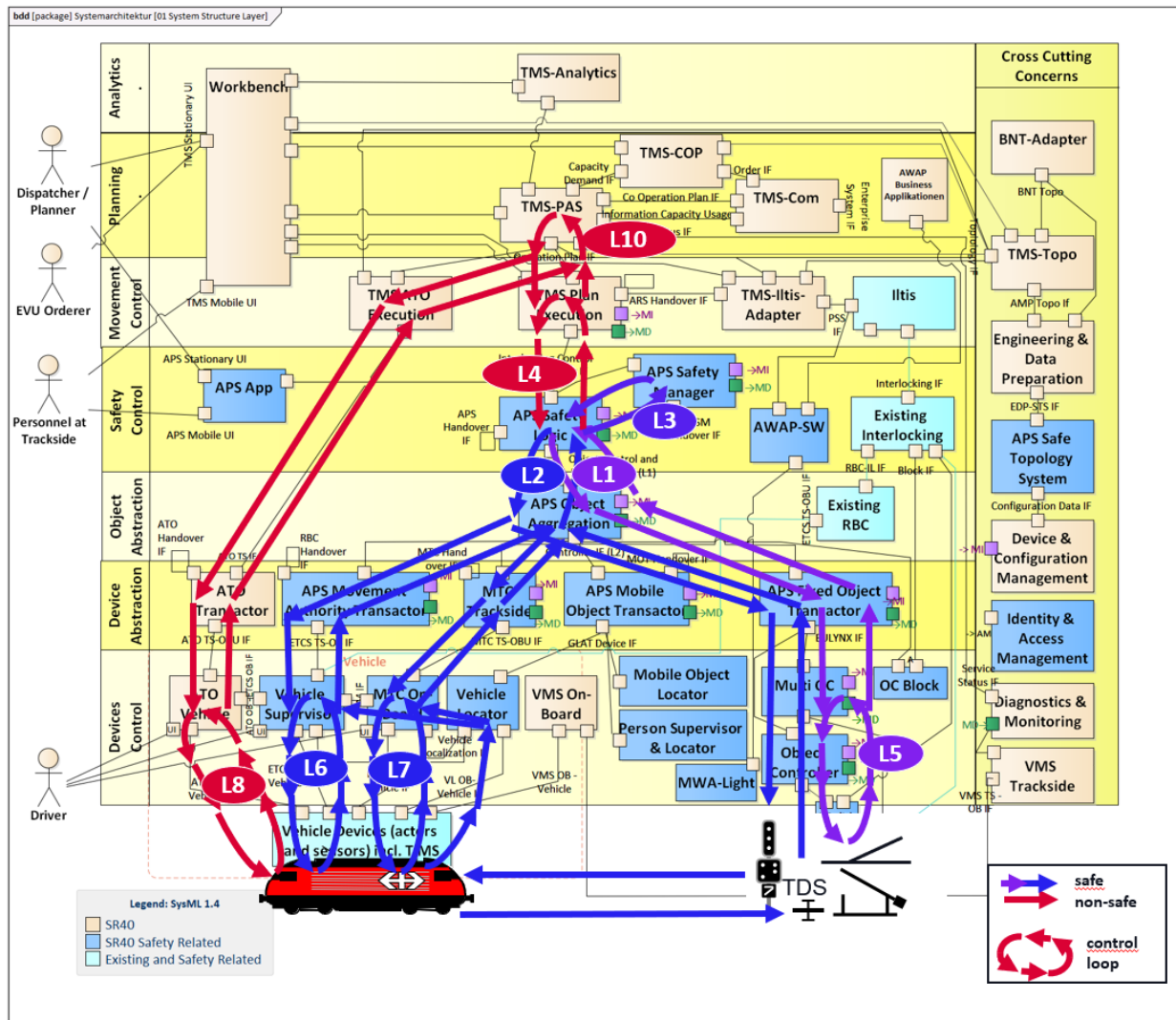

	Prescribed State	Effective State
Vehicle (or group of vehicle)	🗎 WI-1974 - Movement Permission defines a path and a speed profil along the topology, where and how fast a vehicle/vehicle group is allowed to move.	The current location (extend) of the train and its speed.
🗎 WI-6947 - Drive Protection Section (Points, Level Crossing)	Prescribed state of the 🗎 WI-6947 - Drive Protection Section.	The current state of the 🗎 WI-6947 - Drive Protection Section.

The function of the ⬡ SRP-3066 - APS Safety Logic also requires the definition of the topology with its properties. The use of the topology can be restricted by 🗎 WI-1996 - Usage Restriction Areas, which can be added, modified or deleted.

SRP-3066 - APS Safety Logic only allows modification at the WI-1974 - Movement Permission, prescribed state of the WI-6947 - Drive Protection Section and WI-1996 - Usage Restriction Areas if the change is safe.

This following view shows the main control loops for controlling the vehicles and the trackside assets in detail:

L1: Interplay between:

- SRP-3066 - APS Safety Logic prescribes state: State of WI-6947 - Drive Protection Section
- "Real world" (as seen by the device controllers): has effective state of the WI-6947 - Drive Protection Section, which must comply with prescribed state.

Downward: Demanded state of WI-6947 - Drive Protection Section
Upward: Effective state of WI-6947 - Drive Protection Section

L2: Interplay between:

- SRP-3066 - APS Safety Logic prescribes state: Grant specific WI-1974 - Movement Permission to a Moveable Object;
- "Real world" (as seen by the device controllers): effective location, which must comply with prescribed state.

Downward: WI-1974 - Movement Permission (permission to change location).
Upward: Effective location of the Moveable Object in the real world.

Note: There are multiple paths for detecting the location (TPR from vehicle or trackside TDS) and granting the Movement Permission (ETCS L2/L3 or light signals).

L3: Interplay between

- SRP-3066 - APS Safety Logic providing the current state.
- SRP-3069 - APS Safety Manager monitoring the state of the system, such that it can recognize patterns that are identifying hazardous situations and triggering the corresponding safety reactions.

Downward: Requests for changing the state of a WI-6947 - Drive Protection Section or for requesting WI-1974 - Movement Permission.

Upward: State regarding WI-2036 - Movable Objects, WI-1974 - Movement Permission,, WI-6947 - Drive Protection Section, and WI-1996 - Usage Restriction Areas.

L4: Interplay between:

- SRP-3086 - TMS Plan Execution, decomposing the operation plan from SRP-3087 - TMS-PAS into single requests for changing the state of a WI-6947 - Drive Protection Section and for requesting WI-1974 - Movement Permission, issued when all the preconditions regarding the state of the WI-6947 - Drive Protection Section and the "location of the moveable objects" are met;
- SRP-3066 - APS Safety Logic, ensuring SRP-3086 - TMS Plan Execution requests are safely executable and controlling their execution, updating SRP-3086 - TMS Plan Execution with the "effective state of the WI-6947 - Drive Protection Section" and the "location of the moveable objects".

Downward: Requests for changing the state of a WI-6947 - Drive Protection Section or for requesting WI-1974 - Movement Permission.

Upward: "effective state of the WI-6947 - Drive Protection Section" and the "location of the moveable objects".

L5: Local Control Loop between the SRP-3072 - Object Controller and the real trackside asset.

L6: Local Control Loop between the SRP-3081 - Vehicle Supervisor, SRP-3077 - Vehicle Locator and the real vehicle. The SRP-3077 - Vehicle Locator determines from the sensor values the location and speed and provides it to the SRP-3081 - Vehicle Supervisor that supervises the current location and speed against the braking curve and issues brake commands if required.

L7: Local Control Loop between the SRP-9992 - MTC On-Board , SRP-3077 - Vehicle Locator and the real vehicle.

This is the same as L6, except that it uses SRP-9992 - MTC On-Board.

L8: Local Control Loop between the SRP-3084 - ATO Vehicle and the vehicle. The SRP-3084 - ATO Vehicle controls the traction and the brakes to automatically drive the train.

L10 Interplay between:

- SRP-3087 - TMS-PAS, where an WI-2248 - Operation Plan is established (and frequently updated / optimized);
- SRP-3086 - TMS Plan Execution and SRP-3085 - TMS ATO Execution executing the WI-2248 - Operation Plan as faithfully as possible and updating SRP-3087 - TMS-PAS with "real-world" information by providing an execution status.

4 Open Points

The following points are currently open and will bee solved in a later version:

- Time Synchronization

  How is the time synchronized between the different parts of the system, including vehicle and on-board synchronized

- DCM for Vehicle

  Define how the Device and Configuration Management is done for the components on the vehicle.

- IAM Interaction

  Define what mechanism is used for IAM and with which component the IAM communicates.

- External Interfaces

  Show in a separate view where the external interfaces like energy, tunnel automatisation, sensors and ZKE are connected.

5 References

Title	Description	Link
ATO over ETCS SUBSET-126 ATO-OB / ATO-TS Interface Specification	ATO over ETCS SUBSET-126 ATO-OB / ATO-TS Interface Specification	
ATO over ETCS SUBSET-130 ATO-OB / ETCS OB Interface Specification	ATO over ETCS SUBSET-130 ATO-OB / ETCS OB Interface Specification	
ATO over ETCS SUBSET-131 ATO-TS / TMS Interface Specification	ATO over ETCS SUBSET-131 ATO-TS / TMS Interface Specification	
ATO over ETCS SUBSET-132 ATO-TS / ATO-TS Interface Specification	ATO over ETCS SUBSET-132 ATO-TS / ATO-TS Interface Specification	
ATO over ETCS SUBSET-139 ATO-OB / Vehicle Interface Specification	ATO over ETCS SUBSET-139 ATO-OB / Vehicle Interface Specification	
ERTMS SUBSET-026 System Requirements Specification	ERTMS SUBSET-026 System Requirements Specification	
ERTMS SUBSET-034 Train Interface FIS	ERTMS SUBSET-034 Train Interface FIS	
ERTMS SUBSET-037 EuroRadio FIS	ERTMS SUBSET-037 EuroRadio FIS	
ERTMS SUBSET-039 FIS for the RBC/RBC Handover	ERTMS SUBSET-039 FIS for the RBC/RBC Handover	
ERTMS SUBSET-098 RBC-RBC Safe Communication Interface		
UIC O-8664	UIC O-8664, Version 1.0.0, ETCS in	https%3A%2F%2Fuic.org%2FIMG%2Fpdf%2

PS-mode, GPRS/EGPRS Guideline   Fo-8664-1.0.0_etcs_in_ps-mode_gprs-egprs_guideline.pdf

6 Glossary

Term	Abbrev.	Description
Capacity Object		The capacity object is a usage of the capacity to carry out a transport service or a Railway Undertaking (RU)-offer. A capacity object can be: • WI-2400 - Train Run • WI-2402 - Shunting Movement • WI-2403 - Stabling
Capacity Plan		The Capacity Plan determines and balances capacity supply and capacity demand. Capacity planning supports long-term rough planning, medium-term planning and short-term detailed planning. The capacity plan forms the basis for WI-2252 - Traffic Plan and WI-2248 - Operation Plan.
Capacity Restriction		The capacity restriction is a restriction of the usage of the WI-3265 - Topology resulting from construction, maintenance or inspection work, as well as special environmental events or disturbances.
Drive Protection Section	DPS	A Drive Protection Section is an abstraction of locations on the WI-3998 - Railway Network that may adopt different states due to controllable WI-2164 - Trackside Assets (e.g. points or level crossings). It represents a linear extent on WI-3999 - Track Edges that can be brought to different WI-2496 - Trafficability states or give flank protection.
Engine Driver		The engine driver is a person who drives a railway locomotive.
ExecutionState		The execution state describes how far a WI-2248 - Operation Plan has been executed. See WI-3246 - Umsetzungsstatus
Infrastructure Manager	IM	Any body or undertaking that is responsible in particular for establishing and maintaining railway infrastructure. This may also include the management of infrastructure control and safety systems. The functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or undertakings.
Movable Object	MOB	A Movable Object is the logical representation of a track-bound WI-7832 - Vehicle in the WI-2033 - APS Operating State. A Movable Object is uniquely identifiable and is allocated to a WI-7517 - Track Position within the WI-7665 - APS Range.
Movement Permission	MP	A Movement Permission is an authorization for a track-bound WI-2036 - Movable Object to move in a defined direction and along a defined WI-2013 - Track Path on the WI-3998 - Railway Network. A Movement Permission includes all conditions under which movement of the linked WI-2036 - Movable Object can be considered as safe and which a WI-2036 - Movable Object has to adhere to. A Movement Permission always refers to exactly one WI-2036 - Movable Object.
Operation Plan		The Operation Plan is the detailed plan of all track usage, including WI-2400 - Train Runs, WI-2402 - Shunting Movements, WI-2403 - Stablings and intervals. It is created from the capacity plan including the relevant information for RU and partners as well as the basis for the customer information.

Personnel at Trackside		The employees of the RU or IU that are moving at the track (e.g. trackworker) and are therefore in danger of an accident with Moveable Objects.
Shunting Movement		Movement of individual or coupled traction vehicles with or without pulled or pushed trailer load.
Stabling		The parking of a composition or individual cars on a service siding or in rare cases on a main track.
Train Run		A Train Run is the representation of a single planned train journey immediately before the actual journey starts until its completion.
Usage Restriction Area	URA	A Usage Restriction Area is the logical representation of the temporary operating restrictions of a particular WI-7871 - Track Area in the WI-2033 - APS Operating State. The operating restrictions of an Usage Restriction Area are defined by a set of WI-7870 - Usage Restrictions. A Usage Restriction Area does, for example, guarantee the compliance with all operating restrictions resulting from a construction site (e.g. barrier, direction of traffic agreement, speed restriction).