# RCA



**Reference CCS Architecture**

***An initiative of the ERTMS users group and the EULYNX consortium***

# Concept: Plan Execution

Preliminary issue

Document id: RCA.Doc.47

## Table of Contents

**Version History**

| | | | |
|---|---|---|---|
| 0.1 | 24.06.2021 | René Schönemann, Martin Kemkemer, Jens Wieczorek and other members of the RCA-OPE-Cluster | Preliminary version for RCA BL0 R2 |
| 0.2 | 15.09.2021 | René Schönemann, Martin Kemkemer, Jens Wieczorek, Gabriele Löber, Rouzbeh Boloukian-Roudsari and Marcus Völcker as members of the RCA-OPE-Cluster | Preliminary version for RCA BL0 R3 |
| 0.3 | 30.11.2021 | René Schönemann, Martin Kemkemer, Jens Wieczorek, Gabriele Löber, Rouzbeh Boloukian-Roudsari and Marcus Völcker as members of the RCA-OPE-Cluster | Release version for RCA BL0 R3 |

**Release information**

Basic document information:

RCA.Doc.47

Concept Plan Execution

Cenelec Phase: 1

Version: 0.3 (0.A)

RCA Baseline set: 0

Approval date: 30.11.2021

**Disclaimer**

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. Formal requirements management and change management will be introduced in future iterations. The content may be unfinished, will likely contain errors and can be changed without prior notice.

**Imprint**

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)



Support and Feedback

For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu

# 1. Introduction

## 1.1. Purpose of the document

This document is the system concept of SubSys Plan Execution. It defines the system context of SubSys Plan Execution in RCA. The first part of the document therefore describes the functional scope of SubSys Plan Execution on an abstract level, gives an overview of the system interfaces and the organisational, legal and economic aspect of SubSys Plan Execution.

The second part of the document gives an overview of the envisaged RAMS requirements of SubSys Plan Execution.

## 1.2. Maturity and Related Topics

The concept is still work in progress. Whenever it is already known that a section needs further elaboration, this is marked with red italic notes as this: *This section will be further elaborated in future releases.*

This document does not currently consider the division of the SCI-CMD into SCI-CMD, SCI-OS, SCI-PS as envisaged in the RCA Architecture Poster, because the motivation and working principle of the interface division has not yet been sufficiently described.

## 1.3. Related documents

The following related RCA documents provide further information and build on this concept:

- RCA System Architecture, RCA.Doc.35
- RCA Glossary, RCA.Doc.4
- RCA Domain Knowledge Specification, RCA.Doc.18
- Concept: Standard Communication Interface Operational Plan, RCA.Doc.31
- Concept: Architectural Design for Plan Execution, RCA.Doc.49

# 2. System

## 2.1. Scope

### 2.1.1. Introduction

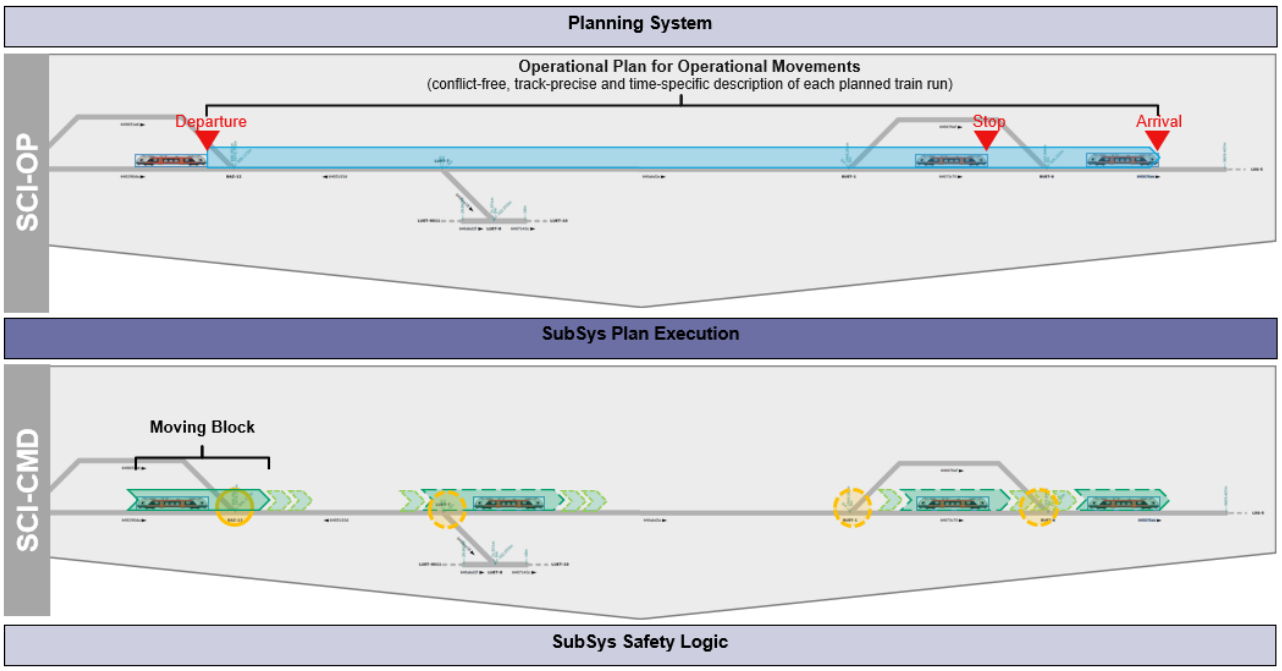


**Figure 1: Illustration of SubSys Plan Execution and the two interfaces SCI-OP and SCI-CMD**

SubSys Plan Execution is a railway control and monitoring system. The core functionality of SubSys Plan Execution is the automatic and efficient execution of the Operational Plans sent by the external Planning System (PAS).

- SubSys Plan Execution implements operational movements by timely requesting Movement Permissions for Physical Train Units and state changes of Field Elements for the driveability of the railway network from SubSys Safety Logic.
- SubSys Plan Execution implements Operational Restriction Areas and Operational Warning Areas by timely requesting these areas from SubSys Safety Logic.
- SubSys Plan Execution considers the dependencies between different Operational Plans as specified by the Planning System.

The final scope of SubSys Plan Execution's functionality is still under consideration.

All of this core functionality is based on the knowledge of the Operating State, a safe logical representation of the actual state of railway operations in the Area of Control, which is provided from SubSys Safety Logic to SubSys Plan Execution via the Standard Communication Interface - Command (SCI-CMD). The Operating State is then processed by SubSys Plan Execution and provided from SubSys Plan Execution to the Planning System outside the system border of RCA via the Standard Communication Interface - Operational Plan (SCI-OP).

As a connecting SubSys between Planning System and SubSys Safety Logic, SubSys Plan Execution makes a decisive contribution to RCA so that the overall system can benefit from new technical possibilities such as precise localisation and integrity check of Physical Train Units, the standardised control of Field Elements and the geometric safety logic of the interlocking.

Characteristics of SubSys Plan Execution:

- operates on abstract representations of real-world elements and objects
- operates in real-time

- functions without need of knowledge about business rules (business rules are expressed in the parameter values of Operational Plans and requests)
- provides functionalities independent of the availability of Planning System (manual input via SubSys Workbench)

### 2.1.2. Objectives and System Requirements

**This section will be further elaborated in future releases**

#### 2.1.2.1. Category: Plan Execution

| Objective PE | System Requirement | Reference to Concept |
|---|---|---|
| O-PE: Ensure the efficient and timely implementation of Operational Plans for Operational Movements, Operational Restrictions and Operational Warning Measures (fully automated)<br><br>O-PE-1.3: Execute Operational Plans considering the operationally needed safety level and the possible risk mitigation measures<br><br>O-PE: Execute Operational Plans by requesting Movement Permissions with any geometric extension.<br><br>O-PE: Implement all functions for the execution of energy-optimal and conflict-free Operating Plans, without support from auxiliary functions of the Planning System or APS<br><br>O-PE: Execution of Operational Plans is based on a generic business logic that can handle the specific capabilities and characteristics of the operated Field Elements and Physical Train Units.<br><br>O-PE: Request the driveability and flank protection state of Field Elements of the railway network to execute Operational Movements<br><br>O-PE: Request Movement Permissions for Physical Train Units to execute Operational Movements | • SubSys Plan Execution shall ensure the efficient und timely implementation of Operational Plans for Operational Movements, Operational Restrictions and Operational Warning Measures (fully automated) sent via SCI-OP or SWI-PE on basis of the activated Map Data, Configuration Data, and the Operating State<br>• SubSys Plan Execution shall constantly monitor the current Operating State<br>• SubSys Plan Execution shall implement the Operational Plans to the earliest point in time possible, but it shall request Movement Permissions and Field Element States only, if immediate needed, so that the Planning System is able the perform a replanning if needed.<br>• SubSys Plan Execution shall calculate the characteristics of the requests optimally to be sent to the SubSys Safety Logic via SCI-CMD to ensure the efficient implementation of Operational Plans<br>• SubSys Plan Execution shall implement the Operational Plans to the earliest point in time possible, but it shall request Movement Permissions and Field Element States only, if immediate needed, so that the Planning System is able the perform a replanning if needed.<br>• SubSys Plan Execution shall optimally trigger the requests to be sent to the SubSys Safety Logic via SCI-CMD to ensure the timely implementation of Operational Plans<br>• SubSys Plan Execution shall enable the closest possible sequence of train movements (moving block)<br>• SubSys Plan Execution shall ensure that trains can run continuously without unwanted stops | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Calculation of MP and triggering of requests via SCI-CMD |
| O-PE: Provide information required for the operation of the RCA system | • SubSys Plan Execution shall execute Operational Plan requested via SCI-OP<br>• SubSys Plan Execution shall provide the Operating State via SCI-OP<br>• SubSys Plan Execution shall provide the Execution State of Operational Plans via SCI-OP<br>• SubSys Plan Execution shall provide the Operating State via SWI-PE<br>• SubSys Plan Execution shall provide the Execution State of Operational Plans via SWI-PE<br>• SubSys Plan Execution shall provide information on its interfaces in such a granularity and format that it is suitable for target systems consuming the information correctly and efficient | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |

| | | |
|---|---|---|
| | • SCI-OP shall allow to request the execution of Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings<br>• SCI-OP shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings<br>• SCI-OP shall allow to request the departure, arrival, or passage times of an Operational Movement<br>• SCI-OP shall allow to request the execution order of different Operational Movements<br>• SCI-OP shall allow to provide the Operating State<br>• SCI-OP shall allow to provide the Execution State of Operational Plans<br>• SCI-OP shall allow to provide the Execution Forecast of Operational Plans<br>• SCI-OP shall allow to provide information in such a granularity and format that it is suitable for RCA external target systems consuming the information correct and efficient | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| | • SWI-PE shall allow to request the execution of Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings<br>• SWI-PE shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings<br>• SWI-PE shall allow to request the precise optimal speed of an Operational Movement<br>• SWI-PE shall allow to request the execution order of different Operational Movements<br>• SWI-PE shall allow to provide the Operating State<br>• SWI-PE shall allow to provide Execution State of Operational Plans<br>• SWI-PE shall allow to provide information in such a granularity and format that it is suitable for SubSys WB | Concept: Standard Workbench Interface Plan Execution, RCA.Doc.xx (TBD) |
| O-PE: Receive and process initial and update requests for Operational Plans | • SubSys Plan Execution shall be able to receive and process initial and update requests for Operational Plans<br>• SubSys Plan Execution shall always know the latest version of an Operational Plan | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Requesting of Operational Plans |
| O-PE: Support handovers of Operational Movements from and to adjacent SubSys Plan Execution | • SubSys Plan Execution shall ensure the efficient and timely handover of Operational Movements from and to adjacent SubSys Plan Execution | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SHI-PE shall allow to request and provide information required for the handover of Operational Movements from and to adjacent SubSys Plan Execution | Concept: Standard Handover Interface Plan Execution, RCA.Doc.xx (TBD) |
| O-PE: Support automated coupling and decoupling of Physical Train Units | • SubSys Plan Execution shall support the automated coupling and decoupling of Physical Train Units | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SCI-OP shall allow to request automated coupling and decoupling of Physical Train Units | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| | • SWI-PE shall allow to request automated coupling and decoupling of Physical Train Units | Concept: Standard Workbench Interface Plan Execution, RCA.Doc.xx (TBD) |
| O-PE: Consider safety rules of SubSys Safety Logic | • SubSys Plan Execution shall consider safety rules of SubSys Safety Logic to successfully issue requests at SCI-CMD | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |

### 2.1.2.2. Category: Robustness

| Objectives PE | System Requirements | Reference to Concept |
|---|---|---|
| O-PE: Handle failures and degraded modes of the railway network efficiently | • SubSys Plan Execution shall report an Execution Failure if a situation in operation cannot be resolved due to the specification of the Operational Plan.<br>• SubSys Plan Execution shall report an Execution Warning if a situation in operation can be neglected but shall be attended due to the specification of the Operational Plan.<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with failures of Field Elements<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with degraded modes of field elements<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with temporary restrictions of the railway network<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with Track Allocations of the railway network<br>• SubSys Plan Execution shall implement retry mechanisms for unsuccessfully executed Operational Events (e.g. in case of stuck field elements)<br>• SubSys Plan Execution shall retry to use the capabilities of the railway network as soon as they are available again. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| O-PE: Handle failures and degraded modes of Physical Train Units efficiently | • SubSys Plan Execution shall report an Execution Failure if a situation in operation cannot be resolved due to the specification of the Operational Plan.<br>• SubSys Plan Execution shall report an Execution Warning if a situation in operation can be neglected but shall be attended due to the specification of the Operational Plan<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with failures of Physical Train Units<br>• SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with degraded modes of Physical Train Units<br>• SubSys Plan Execution shall support the handling of identified, but not safely localized Physical Train Units<br>• SubSys Plan Execution shall support the handling of unidentified but localized Physical Train Units<br>• SubSys Plan Execution shall retry to use the capabilities of the Physical Train Units as soon as they are available again. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| O-PE: Handle failures and degraded modes of the Planning System efficiently | • SubSys Plan Execution shall be able to receive the System State and Operational State of the Planning System and, as a result, take actions to ensure the operation of SubSys Plan Execution, if necessary.<br>• SubSys Plan Execution shall retry to use the capabilities of the Planning System as soon as it is available again. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: System States, Operational States and Modes of Operation |
| | • SubSys Plan Execution shall be able to calculate and check its internal data model for consistency<br>• SubSys Plan Execution shall be able to synchronise the Operational and Configuration Data sent and received via its interfaces | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Robustness and High availability |
| | • SDI shall allow to receive the System State and Operational State of the Planning System | Concept: Standard Diagnostic and Monitoring Interface, RCA.Doc.xx (TBD) |
| | • RCA and its interfaces shall allow to request again the data (operating- and configuration data) already sent and received via the RCA interfaces (event sourcing) | Concept: TBD |

| | | |
|---|---|---|
| O-PE: Handle failures and degraded modes of other RCA SubSys efficiently | • SubSys Plan Execution shall be able to receive the System State and Operational State of other RCA SubSys and, as a result, take actions to ensure the operation of SubSys Plan Execution, if necessary.<br>• SubSys Plan Execution shall retry to use the capabilities of the RCA SubSys as soon as they are available again. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: System States, Operational States and Modes of Operation |
| | • SubSys Plan Execution shall be able to calculate and check its internal data model for consistency.<br>• SubSys Plan Execution shall be able to synchronise the Operational- and Configuration Data send and received via its interfaces | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Robustness and High availability |
| | • SDI shall allow to receive the System State and Operational State of other RCA SubSys | Concept: Standard Diagnostic and Monitoring Interface, RCA.Doc.xx (TBD) |
| | • RCA and its interfaces shall allow to request again the data (operating- and configuration data) already sent and received via the RCA interfaces (event sourcing) | Concept: TBD |
| O-PE: Handle internal failures and degraded modes efficiently | • SubSys Plan Execution shall support different System States, Operational States and Modes of Operation to represent the internal health state and currently supported capabilities of the SubSys Plan Execution<br>• SubSys Plan Execution shall be able to provide its System State and Operational State to other RCA SubSys<br>• SubSys Plan Execution shall be able to provide its System State and Operational State to the Planning System<br>• SubSys Plan Execution shall retry to use its capabilities as soon as they are available again. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: System States, Operational States and Modes of Operation |
| | • SubSys Plan Execution shall be able to calculate and check its internal data model for consistency.<br>• SubSys Plan Execution shall be able to synchronise the Operational- and Configuration Data sent and received via its interfaces | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Robustness and High availability |
| | • SDI shall allow to provide the internal System State and Operational State to other RCA SubSys | Concept: Standard Diagnostic and Monitoring Interface, RCA.Doc.xx (TBD) |
| | • RCA and its interfaces shall allow to request again the data (operating- and configuration data) already sent and received via the RCA interfaces (event sourcing) | Concept: TBD |
| O-PE: Minimize the transfer of safety responsibilities to a human operator even in degraded situations | • SubSys Plan Execution shall minimize the transfer of safety responsibilities to a human operator even in degraded situations | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| O-PE: Allow flexible adaption to data volumes and frequencies without violating the RAMSS specifications | • SubSys Plan Execution shall allow flexible adaption to data volumes and frequencies without violating the RAMSS specifications | Concept: TBD |

| | | |
|---|---|---|
| O-PE: Guarantee high availability (99.95%) | • SubSys Plan Execution shall support different System States, Operational States and Modes of Operation to represent the internal health state and currently supported capabilities of the SubSys Plan Execution<br>• SubSys Plan Execution shall support availability through redundant system instances and hot standby mechanisms<br>• SubSys Plan Execution shall be able to calculate and check its internal data model for consistency.<br>• SubSys Plan Execution shall be able to synchronise the Operational- and Configuration Data sent and received via its interfaces | Concept: TBD |
| O-PE: Act as a temporary fallback level of the Planning System | • SubSys Plan Execution shall implement the functionality to operate APS in case of temporary failure of the Planning System based on information sent and received via SWI-PE by SubSys WB<br>• SubSys Plan Execution shall be able to cache requested Operational Plans and execute them at the sufficient point in time | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SWI-PE shall support manual operation of RCA by SubSys WB | Concept: Standard Workbench Interface Plan Execution, RCA.Doc.xx (TBD) |

| **Objectives A.P.M** | **System Requirements** | **Reference to Concept** |
|---|---|---|
| A.P.M.@Handle internal failures and degraded modes efficiently | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Malfunctioning of system components shall not lead to a shutdown of the system | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Several modes for degraded operation ensuring a high-level of safety and a high-level of operational system must be implemented by design | • System Requirements: TBD | Concept: TBD |
| A.P.M.@The overall system should be as robust as possible against version changes and missing information | • System Requirements: TBD | Concept: TBD |

#### 2.1.2.3. Category: Migration Strategy

| **Objectives PE** | **System Requirements** | **Reference to Concept** |
|---|---|---|
| O-PE: Support the segmentation of the Area of Control of the Planning System | • SubSys Plan Execution shall support the implementation of Operational Plans which overlap its own Area of Control<br>• SubSys Plan Execution shall ensure the efficient and timely handover of Operational Movements from and to adjacent SubSys Plan Execution via SHI-PE | Concept: TBD |
| O-PE: Support migration for existing CTC Systems | • SCI-OP shall support dedicated migration options by supporting existing CTC Systems.<br>• SWI-PE shall support dedicated migration options by supporting existing CTC Systems<br>• SCI-OP shall be independent from operational processes<br>• SCI-OP shall be support different kinds and granularities of Operational Plans independent from provided functionality and behaviour of the Physical Train Units and Field Elements<br>• SubSys Plan Execution shall ensure the efficient and timely handover of Operational Movements from and to adjacent legacy CTC Systems | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| | • SubSys Plan Execution shall implement functionality to support different expansion stages of Planning Systems | Concept: TBD |

| | | |
|---|---|---|
| O-PE: Support migration for different expansion stages of Planning Systems | • SCI-OP shall support different expansion stages of Planning Systems | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| O-PE: Provide functionality to operate APS fully automated, half automated or manually | • SubSys Plan Execution shall provide the functionality to operate APS based on information sent and received via SCI-OP by the Planning System<br>• SubSys Plan Execution shall provide the functionality to operate APS based on information sent and received via SWI-PE by SubSys WB<br>• SubSys Plan Execution bridges the gap between the Operational Plan send by the Planning System via SCI-OP and the simpler commands send to SubSys Safety Logic via SCI-CMD. | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| O-PE: Guarantee railway operation with a mixed ETCS level approach (L2/HL3/L3) of trains and rail network | • SubSys Plan Execution shall guarantee railway operation with a mixed ETCS level approach (L2/HL3/L3) of trains and railway network | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| O-PE: Support different ATO levels (GoA1 – GoA4) and ETCS levels (L2/HL3/L3) | • SCI-OP shall support different ATO levels (GoA1 – GoA4) and ETCS levels (L2/HL3/L3) | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| O-PE: Support the adaptability of business logic to national specific operating rules | • SubSys Plan Execution shall support the adaptability of its business logic to national specific operating rules | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SMI shall be able to provide national specific operating rules | Concept: Standard Maintenance Interface, RCA.Doc.xx (TBD) |
| O-PE: Support standalone usage of ATO without A.P.M. | • SCI-OP shall support standalone usage of ATO without A.P.M. | Concept: Standard Communication Interface Operational Plan, RCA.Doc.31 |
| O-PE: Support handovers of Operational Movements from and to adjacent legacy CTC systems | • SubSys Plan Execution shall ensure the efficient and timely handover of Operational Movements from and to adjacent legacy CTC Systems | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SHI-PE shall support the handover of Operational Movements from and to adjacent legacy CTC Systems | Concept: Standard Handover Interface – Plan Execution, RCA.Doc.xx (TBD) |
| O-PE: Support operation of an entire geographical rollout segment | • SubSys Plan Execution shall be able to operate as a single active instance for an entire geographical segment which includes today multiple interlockings | Concept: TBD |

| **Objectives A.P.M** | **System Requirements** | **Reference to Concept** |
|---|---|---|
| A.P.M.@Allow different system layouts from decentralized to highly centralized safe computing with virtualization and container technologies, n-modular redundancy, fast disaster recovery, multi-tenant and multi-company cloud structures | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Avoid temporary investments (e.g. avoid temporary interfaces between old and new interlockings by supporting technically the efficient and stable replacement of full lines by just replacing safety logic but not the OC) | • System Requirements: TBD | Concept: TBD |

| | | |
|---|---|---|
| A.P.M.@Provide scalable system architecture to be used in a modular way depending on local needs | • System Requirements: TBD | Concept: TBD |

### 2.1.2.4. Category: RAM Strategy

| Objectives PE | System Requirements | Reference to Concept |
|---|---|---|
| O-PE: Reduce the RAMS requirements of the Planning System | • SubSys Plan Execution shall implement dedicated functionality to reduce the RAMS requirements of the Planning System | Concept: TBD |

| Objectives A.P.M | System Requirements | Reference to Concept |
|---|---|---|
| A.P.M.@Architecture design reduces the functional and non-functional dependencies between the SubSys and thus reduces the functional and non-functional requirements (especially RAMS) for the individual SubSys. | • SubSys Plan Execution shall achieve No SIL or SIL 0<br>• SubSys Plan Execution shall be highly available | Concept: TBD |
| A.P.M.@Demonstrably successful best practices in software development for highly available systems should be applied | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Provide data about system behaviour about RAMS and capacity usage to other systems | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Reduce maintenance efforts by maximally reducing dependencies between building blocks | • System Requirements: TBD | Concept: TBD |

### 2.1.2.5. Category: Safety Strategy

| Objectives PE | System Requirements | Reference to Concept |
|---|---|---|
| O-PE: Develop RCA SubSys according to EN 50128 | • SubSys Plan Execution shall be developed according to EN 50128 | Concept: TBD |
| O-PE: Achieve the most extensive generic safety assurance possible while minimising the scope of the specific safety assurance | • SubSys Plan Execution shall achieve the most extensive generic safety assurance and shall therefore be able to be approved independently of specific engineering data or HW specifications | Concept: TBD |
| O-PE: Implement specific unscheduled manual operations which require up to SIL 2 within GUI-Application of SubSys WB (stationary or mobile) separated via SWI-PE from SubSys Plan Execution | • SubSys Plan Execution shall implement specific unplanned manual operations which require up to SIL 2 within GUI-Application of SubSys WB (stationary or mobile)<br>• SWI-PE shall allow to request the execution of specific unscheduled manual operations which require up to SIL 2<br>• SWI-PE shall provide information required to implement specific unscheduled manual operations which require up to SIL 2 in SubSys WB | Concept: Standard Workbench Interface Plan Execution, RCA.Doc.xx (TBD) |

| Objectives A.P.M | System Requirements | Reference to Concept |
|---|---|---|
| A.P.M.@Apply a generic safety approach in encapsulating smallest possible safety relevant functions in building blocks that allow a separate safety assurance | • System Requirements: TBD | Concept: TBD |

| | | |
|---|---|---|
| A.P.M.@Design a modular system architecture with small as possible amount of safety relevant components | • System Requirements: TBD | Concept: TBD |

### 2.1.2.6. Category: Security Strategy

| Objectives A.P.M | System Requirements | Reference to Concept |
|---|---|---|
| A.P.M.@Avoid unnecessary authorisation by building trusted clusters | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Ensure security by design for all SubSys and data flows according to RCA | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Support the integration with state of the art identity and access management service | • System Requirements: TBD | Concept: TBD |

### 2.1.2.7. Category: Life Cycle Management and Updateability

| Objectives PE | System Requirements | Reference to Concept |
|---|---|---|
| O-PE: Support independent updateability of HW and SW and Engineering Data | • SubSys Plan Execution shall have a strong separation of SW and HW concerns.<br>• SubSys Plan Execution should have generic application logic that works independently of the content of the Map Data, if the structure of the Map Data is respected | Concept: TBD |
| O-PE: Enable changes, adaptations, and extensions throughout the life cycle of the building blocks | • SubSys Plan Execution shall enable changes, adaptations, and extensions throughout the life cycle of its internal building blocks | Concept: TBD |
| O-PE: Ensure network wide adaptability towards changes of the trackside CCS SubSys | • SubSys Plan Execution shall ensure network wide adaptability towards changes of the trackside CCS SubSys | Concept: TBD |
| O-PE: Allow flexible adaption to data volumes and frequencies without the need to change the code basis | • SubSys Plan Execution shall allow flexible adaption to data volumes and frequencies without the need to change the code basis | Concept: TBD |

| Objectives A.P.M | System Requirements | Reference to Concept |
|---|---|---|
| A.P.M.@Asset management must support the demand for high-cadence asset modification | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Build a modular system architecture that supports different lifecycles | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Enable changes, adaptations and extensions throughout the life cycle of the building blocks | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Exchangeability between building blocks must be present wherever non-overlapping technology lifecycle profiles are present | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Overlapping technology lifecycle profiles must be | • System Requirements: TBD | Concept: TBD |

| | | |
|---|---|---|
| respected by the system design | | |

### 2.1.2.8. Category: Standardisation, Automation, and Integration

| Objectives PE | System Requirements | Reference to Concept |
|---|---|---|
| O-PE: Support efficient and safe update of Map Data Version during runtime | • SubSys Plan Execution shall be able to be operated during a Map Data Version Update<br>• SubSys Plan Execution ensures that the Map Data Version Update is accomplished in the shortest possible time to minimize the unavailability of updated Map Data Elements. | MAP Concept (including MAP Solution Concept PUB-TS) - to be released |
| | | Capability: Activate Map Data |
| | | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br>Functional concept: TBD |
| O-PE: Process (partly automated) alarms regarding hazardous situations<br><br>(currently not defined if in-scope or out-of-scope of SubSys Plan Execution) | • SubSys Plan Execution shall process (partly automated) alarms regarding hazardous situations (e.g. avalanche sensors, hot box detector, short circuit in catenary sections, emergency call of train driver) | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: Alarms regarding hazardous situations |
| O-PE: Support clearly designed and robust interfaces for fully automated data exchange | • SubSys Plan Execution shall use standardised interfaces for communication with other (sub-)systems<br>• SubSys Plan Execution shall not make excessive demands on the complexity of interfaces<br>• SubSys Plan Execution shall support easy adaptable interface for avoiding manual data exchange efforts<br>• SubSys Plan Execution shall be able to handle inaccurate input data and provide helpful error messages on its interfaces in case of incorrect input data | Concept: TBD |
| O-PE: Provide data capturing to enable predictive maintenance | • SubSys Plan Execution shall provide diagnostics data to enable predictive maintenance | Concept: Architectural Design for Plan Execution, RCA.Doc.49<br><br>Functional concept: TBD |
| | • SDI shall support the provisioning of diagnostics data from RCA SubSys | Concept: Standard Diagnostic and Monitoring Interface, RCA.Doc.xx (TBD) |
| O-PE: The building blocks and their interfaces should have as little version dependency as possible | • SubSys Plan Execution shall ensure that its internal building blocks and their interfaces should have as little version dependency as possible | Concept: TBD |
| O-PE: Introduce generic capability-based interfaces | • SubSys Plan Execution shall provide generic capability-based interfaces | Concept: TBD |

| Objectives A.P.M | System Requirements | Reference to Concept |
|---|---|---|
| A.P.M.@Accompanying standardisation to reduce system compatibility testing between onboard and trackside | • System Requirements: TBD | Concept: TBD |
| A.P.M.@All building blocks shall utilise an identical MAP data reference, provided by each MAP data version in order to prevent interpretation efforts | • System Requirements: TBD | Concept: TBD |

| | | |
|---|---|---|
| A.P.M.@Allow large area of control segment sizes to reduce the amount of transitions to neighboring legacy systems in order to reduce integration efforts | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Consider open interfaces to integrate as much formats as possible | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Deployment of the system must be possible in various configurations but all of them need to fulfil basic requirements | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Encapsulate minimal viable functionalities in building blocks to enable an individual configuration of the building blocks and simple interfaces | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Integrate upwards compatibility by design | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Reduce complex and manually triggered or processed process and replace or reengineer with automated processes | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Standardize all main CCS processes, functionalities and interfaces | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Support a broad applicability to different railways and in various types of traffic and operational processes | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Use interfaces with automatic adaptions and internal intelligence for interfacing different versions of building blocks without the need of upgrade existing building blocks based on change in interface | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Use secure standard protocols | • System Requirements: TBD | Concept: TBD |
| A.P.M.@Use standardized processes and systems | • System Requirements: TBD | Concept: TBD |
| A.P:M.@Implement ATO GoA2 or GoA3-4 | • System Requirements: TBD | Concept: TBD |

### 2.1.3. Features

- Efficient and timely implementation of Operational Plans for Operational Movement, Operational Restriction and Operational Warning Measure sent by the Planning System.
    - Requests the driveability of the desired Track Path by sending just-in-time requests to the Safety Logic for each Field Element, based on the operational situation.
    - Requests a Movement Permission for safe operational movement by sending just-in-time request to the Safety Logic with the optimal characteristics, based on the operational situation.
    - Implement Operational Restriction Areas and Operational Warning Areas by sending just-in-time requests to the Safety Logic.
    - Uses the unified data model defined in RCA that represents the railway network.

- Provides information about the execution progress of Operational Plans to the Planning System.
- Processes information about the operational situation received from SubSys Safety Logic and provide this information to the Planning System in near real time.
- Provide information and commands needed for manual operation of SubSys PE via SubSys Workbench (temporary fallback level for the Planning System, unplanned manual interactions).

PE is characterized by very high availability, very low latency and very short and deterministic reaction times.

### 2.1.4. Out of scope

The functions listed are not part of the scope of SubSys Plan Execution, although they are included in current systems such as existing centralized traffic control (CTC) or interlocking systems that are to be replaced by Advanced Protection System (APS) and SubSys Plan Execution. Some of the listed functions have no relevance anymore in the RCA context or they are in the scope of other systems such, as the Panning System. The list is not exhaustive and may still change due to the adapted architecture.

**Operational Plan management**

- PE does not support Operational Plan that offer different variants for the given Track Path from the departure to the arrival position. SubSys Plan Execution only supports track-exact Operational Plans.
- PE does not resolve conflicts between different Operational Plans, nor does it change the order of Operational Movements dictated by the Operational Plans, both aspects are the responsibility of the Planning System.
- PE does not perform route compatibility checks nor will it check whether the vehicle data specified in an Operational Plan for Operational Movement corresponds to the vehicle data reported by Safety Layer. These checks must be done by the Planning System or by the Railway Operator (in SubSys Workbench) before the Operational Plan for Operational Movement is sent to SubSys Plan Execution. SubSys Plan Execution will implement the Operational Plan although there might be incompatibilities between the properties of the planned train unit and the physical train unit or between the properties of the planned / physical train unit and the planned Track Path.

**Driveability management**

- SubSys Plan Execution does not handle any manually or locally operated Field Elements, which do not have a technical interface to APS. This means that e.g. manually operated points or level crossings in the Area of Control must either be replaced by automated ones or must be handled by IM specific operational processes.
- SubSys Plan Execution does not support monitoring and control of catenary sections. Catenary sections must continue to be supported by the responsible systems outside of RCA.

**Operational Movement management**

- **Movement Permission**
    - SubSys Plan Execution does not support classic track route principles as todays interlockings (request a track route and the required conditions of e.g. Field Elements are configured in the interlocking). With SubSys Plan Execution the driveability of the Track Path and the Movement Permission including the Risk Buffer and the Risk Paths are requested separately. Fixed block lengths are no longer required. Each request send by SubSys Plan Execution to SubSys Safety Logic is checked by SubSys Safety Logic regarding the safety rules.
- **Deadlock detection**
    - SubSys Plan Execution does not provide any kind of deadlock detection to prevent overfilling of the railway network, this functionality must be provided by the Planning System.
- **Shunting**
    - SubSys Plan Execution does not distinguish train runs and shunting movements as todays interlockings. Any movement of a Physical Train Unit is either planned and processed as Operational Movements in an Operational Plan or is not supported.

**Operational Warning Measure management**

- **Warning**
  - SubSys Plan Execution does not track or process the current position, properties and state of non-track bound vehicles, trackside personal or warning devices.
  - SubSys Plan Execution is not responsible for matching warning devices to Operational Warning Areas or setting up warning devices
  - SubSys Plan Execution does not trigger actual warnings for warning devices to warn Physical Train Units, non-track-bound vehicles or trackside persons within or close to a warning area.

### 2.1.5. Overview of functionalities

**Functionalities of SubSys Plan Execution:**

- **Plan execution**
  - **Operational Plan management**
    - Function: Process Operational Plan
- **Automatic plan execution**
  - **Driveability management**
    - Function: Observe driveability of railway network
    - Function: Provide driveability of railway network
    - Function: Control driveability of railway network
      - Subfunction: Calculation of Trigger Points for driveability requests
  - **Operational Movement management**
    - Function: Observe Operational Movement of Physical Train Units
    - Function: Provide Operational Movement of Physical Train Units
    - Function: Control Operational Movement of Physical Train Units
      - Subfunction: Calculation of MP
      - Subfunction: Calculation of Risk Buffer
      - Subfunction: Calculation of Risk Paths
      - Subfunction: Calculation of Trigger Points for MP requests
  - **Operational Restriction management**
    - Function: Observe Usage Restriction Areas on railway network
    - Function: Provide Operational Restriction Areas on railway network
    - Function: Control Operational Restriction Areas on railway network
  - **Operational Warning Measure management**
    - Function: Observe Warning Areas on railway network
    - Function: Provide Operational Warning Areas on railway network
    - Function: Control Operational Warning Areas on railway network
- **Manual plan execution**
  - Function: Manual plan execution
- **Device and Configuration Management**
  - Function: Import Configuration Data
  - Function: Activate Map Data
- **Monitoring and Diagnostics**
  - Function: Send diagnostics data
- **Authentication and Authorisation**
  - Function: Use authentication and authorisation services
- **Robustness**
  - Function: Support different System States, Operational States and Modes of Operation
  - Function: Determine System- / Operational State
  - Function: Provide and receive System- / Operational State
  - Function: Calculate and check internal data model
  - Function: Synchronise the state of Configuration Data and Operational Data

## 2.2. Context

### 2.2.1. RCA

- SubSys Plan Execution is specified in the RCA. In terms of the overall RCA it is a SubSys.
- SubSys Plan Execution is specified as a product.
- SubSys Plan Execution is envisaged as a non-safety-relevant system.
- The development process should be done according to EN 50126-1 and EN 50128 anyway, as one must develop according to these standards from SIL 0. The actual SIL requirements will be determined on basis of the required risk analysis.
- As part of RCA the SubSys Plan Execution is intended for international use by European railway Infrastructure Managers.
- SubSys Plan Execution is specified synchronously with other SubSys such as APS in the RCA and is connected to adjacent SubSys via defined interfaces.
- With the SCI-OP, SubSys Plan Execution provides the interface that defines the system boundary from RCA to the Planning System.
- For the development of SubSys Plan Execution and it's interfaces the compliance with international standards (e.g. TSI TAF/TAP, RailML) is to be observed.
- SubSys Plan Execution is designed as a highly available system.
- SubSys Plan Execution is operated together with exactly one logical instance of a Planning System and exactly one logical instance of APS. (However, a Planning System should be able to operate multiple logical RCA system instances simultaneously to divide the entire operational area of PAS into multiple Areas of Control each handled by a single RCA systems, thus achieving scalability).
- SubSys Plan Execution has an interface (SHI-PE) to other neighbouring SubSys Plan Execution to work in a joint network.

### 2.2.2. Operation and training

- For the operation of SubSys Plan Execution, an operating concept must be available.
    - The operating concept defines responsibilities and procedures between all organisations involved.
    - Service Level Agreements define which services are provided and by whom.
    - All measures and solutions affecting operation must be coordinated with the licensee and laid down in the operating concept.
- In case of detected errors or failures during operation, the state must be recorded.
    - It is recorded when an error occurs, when the error was eliminated and since when SubSys Plan Execution has been in operation again.
- Before handing over the system, the system operator and the personnel must be trained in the parts of the system relevant to them.

### 2.2.3. Organisation

- SubSys Plan Execution supports generic concepts and can therefore be used independently of the operational organisation or exact operational use within the limits of the scope of the system.
- SubSys Plan Execution shall not have any additional and specific restrictive effects on the organisation, neither by the possible number of workplaces, their local distribution across sites or distribution in a site, nor by the operational concept (administration, monitoring, maintenance).

## 2.3. Environment

### 2.3.1. Physical influences

SubSys Plan Execution consists of hardware and software. The hardware component is exposed to physical influences. The technical system, SubSys Plan Execution, runs on a computer platform (not yet specified).

The application, SubSys Plan Execution, is also manually used by the Railway Operators via SubSys Workbench from suitable workstations and on mobile devices. Physical influences and restrictions therefore refer to the computer platform and the hardware used at the stationary and mobile workplace.

### 2.3.2. System interfaces

SubSys Plan Execution interacts with internal and external SubSys over distinct interfaces. For all interfaces, detailed interface concepts and specifications either exist or are planned. The following sections describe therefore only in brief the interfaces from and to SubSys Plan Execution.

#### 2.3.2.1. SCI-OP

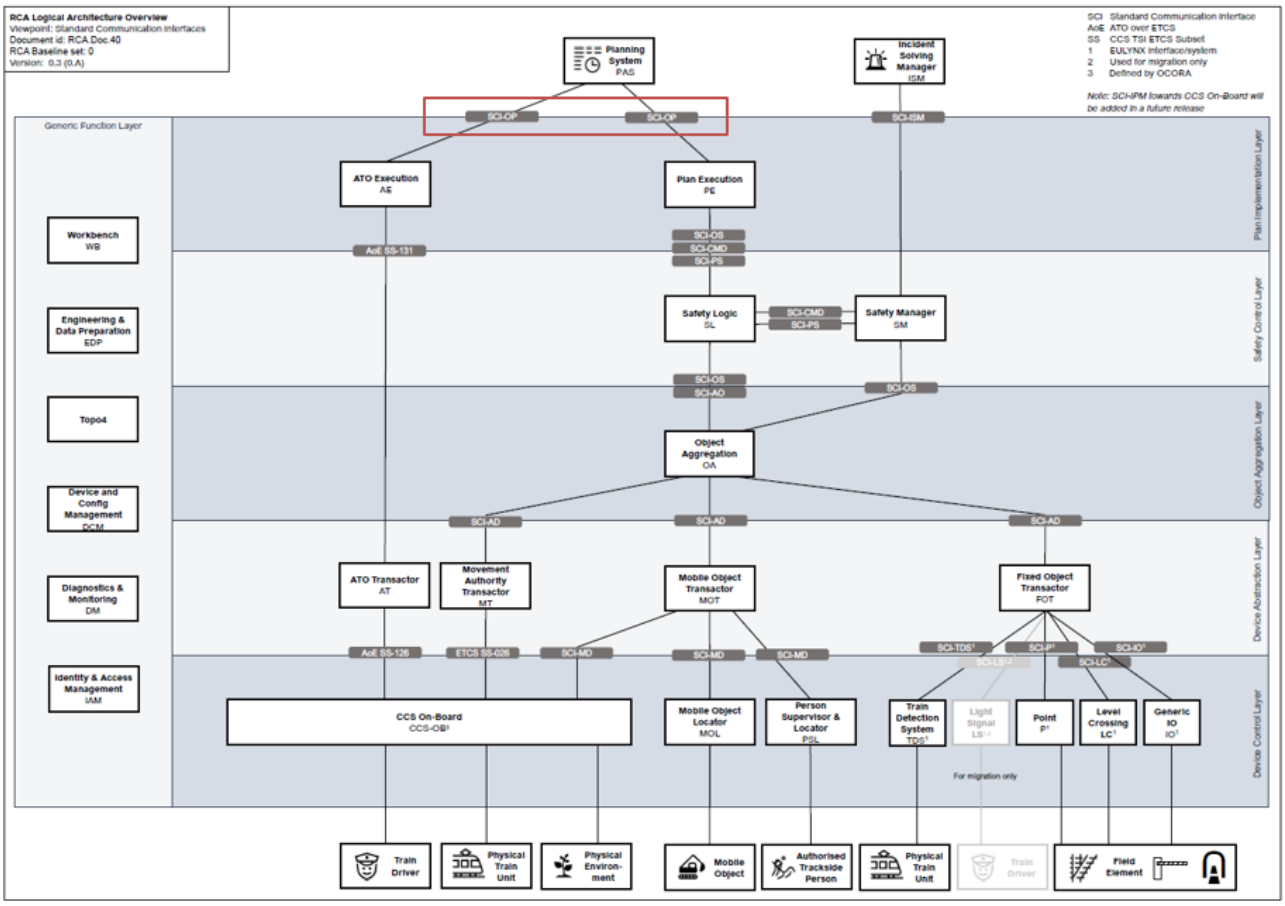


**Figure 2: SCI-OP in the RCA Logical Architecture**

**Description of SCI-OP**

- **Full name:** Standard Communication Interface - Operational Plan
- **Description:**
  - The SCI-OP is part of the Reference CCS Architecture. SCI-OP is on the RCA system border between the Planning System and the RCA SubSys ATO Execution and Plan Execution. The Planning System sends Operational Plans via the SCI-OP to be implemented by ATO Execution and Plan Execution. ATO Execution and Plan Execution will provide information about the execution progress of the Operational Plans (Operational Plan Execution) and the actual state of railway operations in the Area of Control (Operating State).
- **Downstream:**
  - Request Operational Plan of type Operational Movement, Operational Restriction, Operational Warning Measure (entity: Operational Plan Execution Request)
- **Upstream:**
  - Provide Operational Plan Execution (entities: Operational Plan Execution Response, Operational Plan Execution Report, Operational Plan Execution Forecast)

- Provide Operating State (entities: Train Unit Report, Track Allocation, Operational Restriction Area, Operational Warning Area, Field Element State)

### 2.3.2.2. SCI-CMD

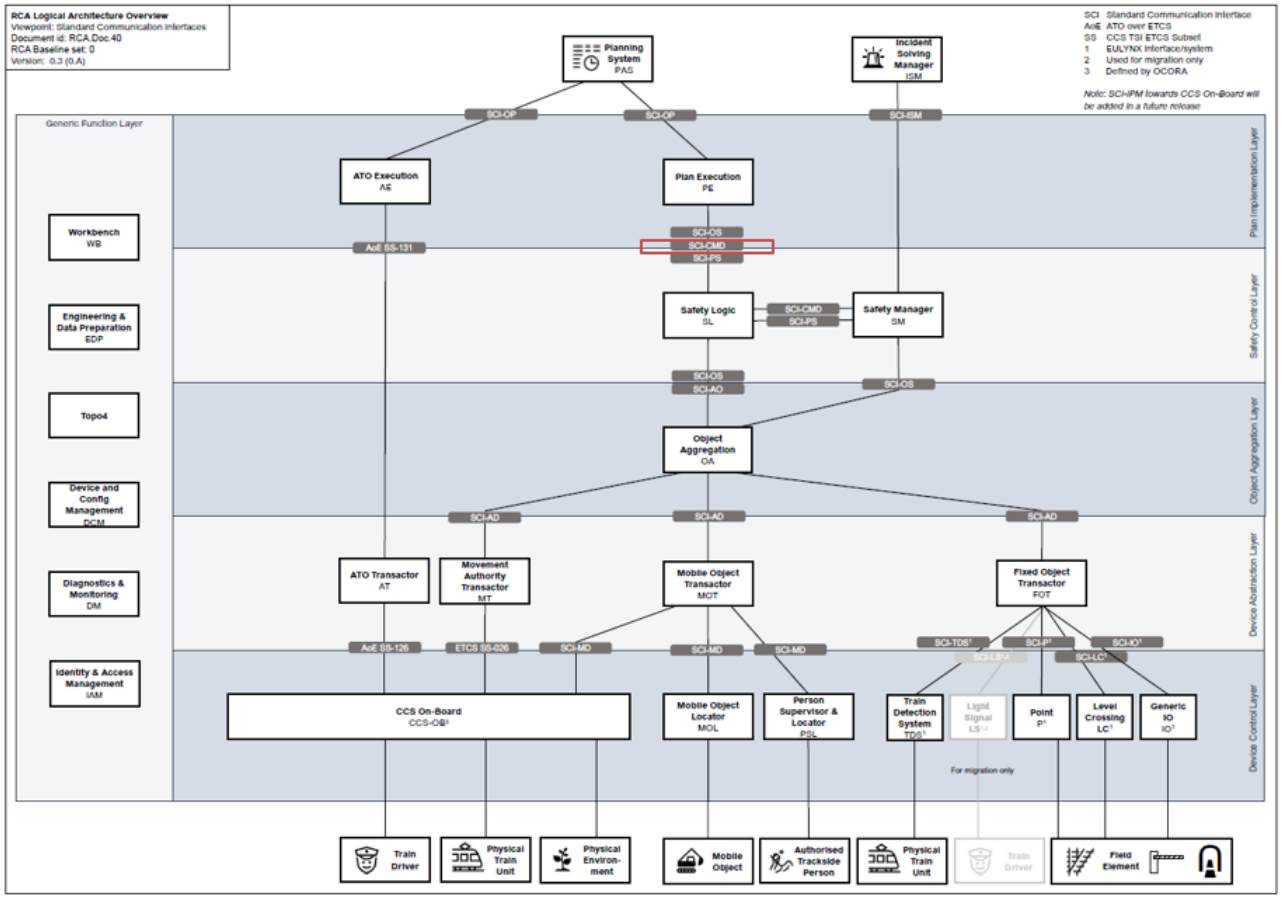


**Figure 3: SCI-CMD in the RCA Logical Architecture**

**Description of SCI-CMD**

- Description is in responsibility of APS-Cluster.
  Please refer to RCA System Architecture, RCA.Doc.35, for details.

### 2.3.2.3. SWI-PE

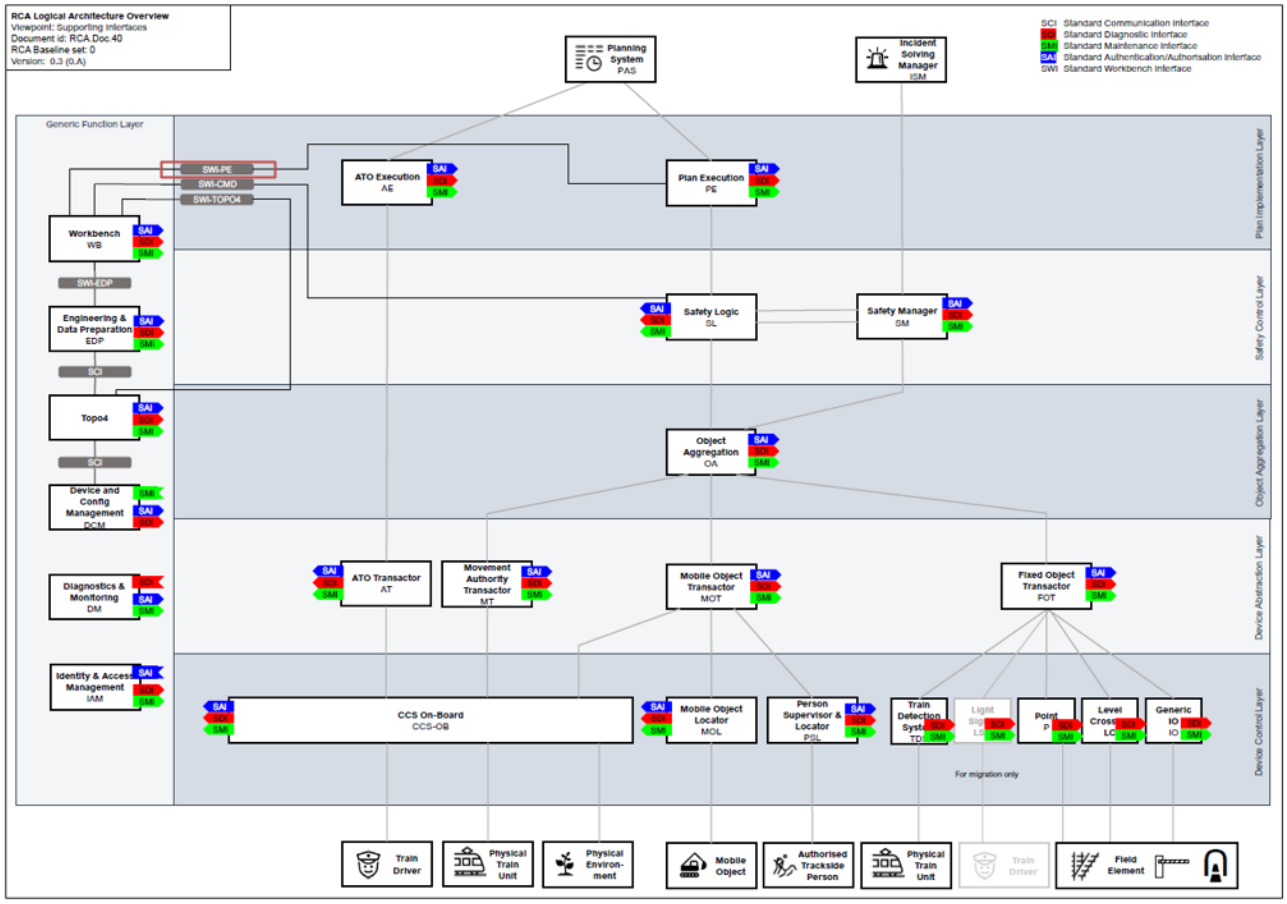


**Figure 4: SWI-PE in the RCA Logical Architecture**

**Description of SWI-PE**

- **Full name:** Standard Workbench Interface – Plan Execution
- **Description:**
  - The interface defines the communication standard between the SubSys Workbench and SubSys Plan Execution. It provides input/output functions for user interactions with SubSys Plan Execution (e.g. unplanned manual activities, fallback level for the Planning System). The interface must support a stationary as well as a mobile user interface. The latter shall provide the user interaction for the Authorized Trackside Persons including but not limited to the input of requests or the display of up-to-date information on the next planned Operational Movements.
- **Downstream:**
  - Request Operational Plan of type Operational Movement, Operational Restriction, Operational Warning Measure (entity: Operational Plan Execution Request)
  - Request unplanned manual object controls
- **Upstream:**
  - Provide Operational Plan Execution (entities: Operational Plan Execution Response, Operational Plan Execution Report, Operational Plan Execution Forecast)
  - Provide Operating State (entities: Train Unit Report, Track Allocation, Operational Restriction Area, Operational Warning Area, Field Element State)

### 2.3.2.4. SHI-PE

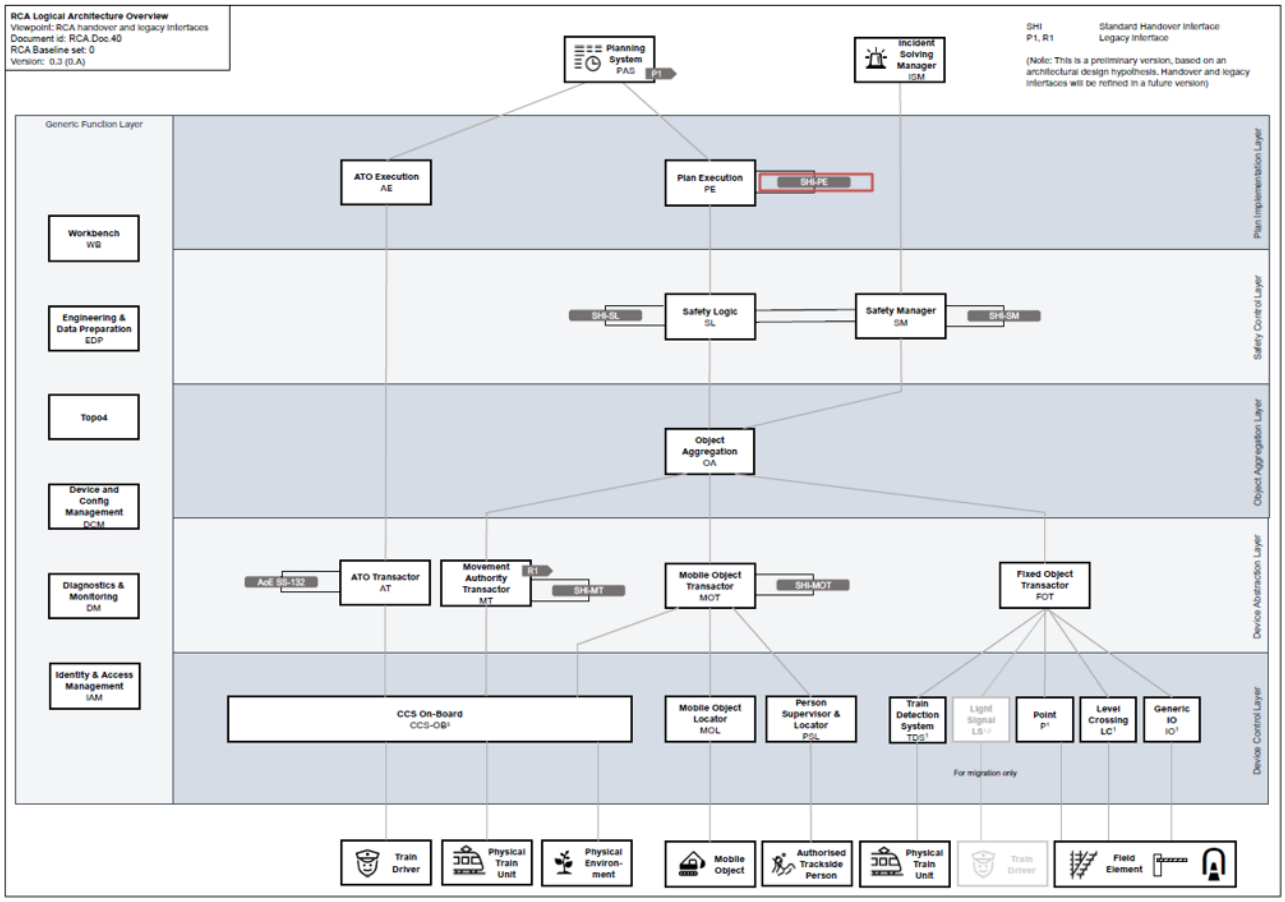


**Figure 5: SHI-PE in the RCA Logical Architecture**

**Description of SHI-PE**

- **Full name:** Standard Handover Interface – Plan Execution
- **Description:**
  - The interface defines the communication standard between two Plan Execution systems. It is used to exchange information about each other's Area of Control and to pass a Physical Train Unit from one Area of Control to the next.

### 2.3.3. Cross sectional system interfaces

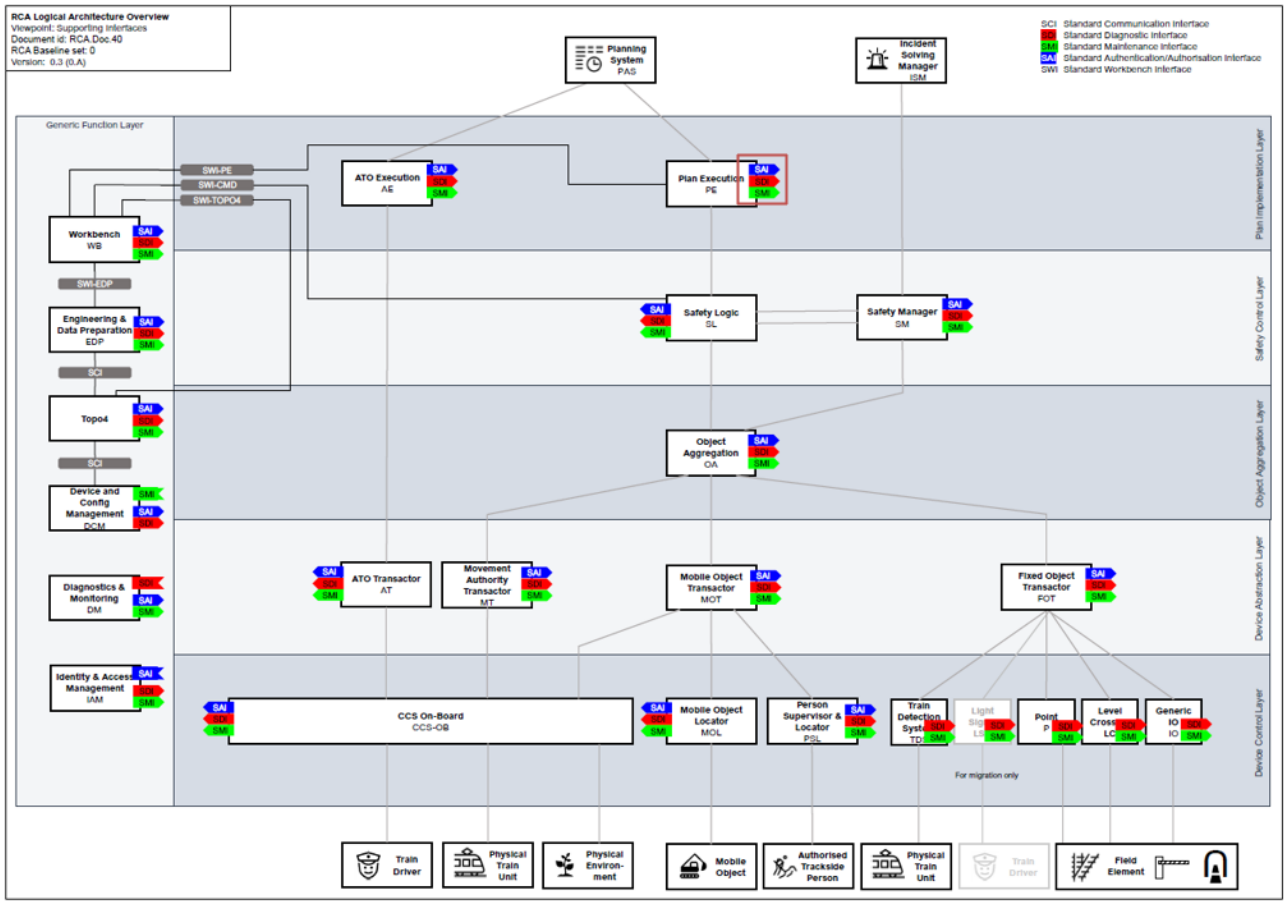


**Figure 6: SMI, SDI, SAI in the RCA Logical Architecture**

#### 2.3.3.1. SMI

**Description of SMI**

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA System Architecture, RCA.Doc.35, for details.

#### 2.3.3.2. SDI

**Description of SDI**

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA System Architecture, RCA.Doc.35, for details.

#### 2.3.3.3. SAI

**Description of SAI**

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA System Architecture, RCA.Doc.35, for details.

### 2.3.4. Economic and legal aspects

Legal aspects concern:

1. Occupational safety e.g. for usability graphical user interfaces
2. Signalling safety ("safety")
3. Information security ("security")
4. Product liability, e.g. due to traceability aspects

SubSys Plan Execution as other RCA SubSys is intended for international use. A reference to the legal basis will be made as soon as the countries in which SubSys Plan Execution is used are known. More details on safety can be found in chapter Safety Legislation 3.3.

Economic aspects are not dealt with at this point.

# 3. RAMSS

## 3.1. RAMSS Performance and Requirements

The following subchapters list the initial performance and requirements regarding Reliability, Availability, Maintainability, Safety and Security for SubSys Plan Execution.

### 3.1.1. Reliability

SubSys Plan Execution is a reactive system. It interacts continuously in real time with other systems and the behaviour is driven by the transmitted data. The input is processed immediately, and the results are propagated. The processing must happen during well-defined response time. If SubSys Plan Execution works without high reliability, the reliability of the consuming systems can be affected as well.

Software reliability is given by the probability that a specific program performs fault free during a defined time period and in a defined environment. This means, software reliability is a software metric and can be measured or estimated by objective criteria. The metric is the ratio between the number of successful passed test cases and the number of overall test cases. During the validation phase this ratio shall be 1.

It is not possible to write fault free software and even in the final version it is likely to find remaining systematic faults, even if all tests were performed successfully. During operation, the FRACAS system will observe the operation permanently and the reported reliability index (fault free calculations divided by all calculations) shall be very close to 1.

The number of test cases and the coverage of test cases must be defined well as part of the validation plan. The principle to find the correct number of test cases must be explained and should make use of static code analyses ensure that all branches in the software are covered. A test management and test performing tool shall be used.

It's fundamental for SubSys Plan Execution that at least these areas are covered by the reliability testing:

- Correctness, meaning all calculations are free of faults and only verified data, valid for consuming systems, are propagated.
- Concurrency, meaning that calculation can be processed in parallel. This is a precondition for scalability. SubSys Plan Execution needs to be able to process concurrent requests from the Planning System and SubSys Workbench. Concurrency includes not only independent requests (e.g. independent due to different train numbers or disjoint geography) but also dependent requests.
- Resistance against:
    - Failures caused by inconsistent or incomplete input data from systems or human input.
    - Software faults (fault tolerant reaction).
    - Overload of the system.
- Performance and on time response (under various load scenarios).
- Communication, e.g. suppression of double sent messages.
- Elasticity, meaning to scale with various data volumes and data frequencies while response time stays in defined boundaries.

Furthermore, the reliability shall be assured by results of static software analyses. Details of the metric to use are given the software validation plan.
For SubSys Plan Execution, the reliability planning and test planning -covering theses aspects- will be outlined in the validation plan. After reliability testing a reliability prediction can be made by the validation report. During system operation FRACAS will perform reliability data acquisition reliability analysis.

### 3.1.2. Availability

System availability depends on hardware and software availability. This chapter is dealing with software availability while hardware availability should be covered by overall RCA RAM documents. Software availability can be measured during system operation. The quantitative prediction of software availability cannot be done seriously at this stage.

In principal, the availability depends on the reliability, a higher reliability leads to a higher availability. But even with the highest reliability you can and will have systematic faults in the software, causing failures.

Ensuring highest availability leads to strategies how to react fault tolerant in case of faults.

Availability is the ratio of the duration of fault free operation (up time) divided by the agreed operational time. Two strategies are relevant for SubSys Plan Execution and shall be covered by the software architecture, using proven patterns to design

- fault tolerance reaction (e.g. fail over).
- fault impact (failure) limitation.

This design shall cover detailed analyses of reliability for all software components including operating system, middleware, databases, frameworks and SubSys Plan Execution software itself. If SubSys Plan Execution consists of a micro service architecture, the detailed analyses are required for all independent micro services and for common services.

The impact of failures caused by systematic software faults shall be analysed for all software components (listed above). This shall consider various scenarios of input data. E.g. a fault in the processing of the input data could apply to a single train number only and as a result only a single train is not managed properly. A fault in the output preparation could affect many trains and the impact could be much bigger.

For SubSys Plan Execution software, no quantitative prediction of availability will be made at this moment. Qualitative prediction can be made based on design principles outlined above. Furthermore, SubSys Plan Execution will increase the availability by selecting proven components. Proven means the expected number of undetected systematic software faults is low.

For the selection of COTS (Commercial of-the-shelf) components the project for SubSys Plan Execution shall consider:

- Components with a low complexity are better. A value for an acceptable complexity, based on a standard software metric, will be given in the architecture document.
- Components with longer life cycle (not brand new) and used by a high number of installations are better. A minimum past operating time for each component will be given in the architecture document.
- Components available in source code are better due to static analyses can be executed.
- Components used in similar operating environments are better, not exclusively in the context of railway.

Detailed requirements are given in the software architecture document.
Availability will be measured initially during shadow run under conditions similar to the required operating conditions of existing CTC Systems. During system operation FRACAS will perform availability data acquisition availability analysis.

### 3.1.3. Maintainability

With reliability, SubSys Plan Execution reduces the number of (detected) software faults. The undetected software faults and the impacts are discussed under availability. If an undetected software faults leads to a failure, the fault is now detected and the code can be fixed. Keeping the meantime to repair for these faults very short is one aspect of maintainability. Another aspect is the long-time maintainability, not driven by faults but by features to be implemented in further releases. Good maintainability is important to ensure the software life cycle for short-time and long-time corrections and improvements. While experts (from railway perspective and software engineering perspective) are very limited, good documentation is also an important aspect of maintainability. Like availability and reliability, maintainability is a software metric measurable by objective criteria. The calculation and the mandatory value for SubSys Plan Execution will be given with the validation plan. Good maintainability leads to software design and software implementation aspects as well as to process aspects.
The software architecture document, which outlines the requirements for maintainability are fulfilled, shall cover at least these principles:

- modular design with single modules, to make sure that they can be tested separately.
- usage of proven and broadly accepted design and implementation patterns (best practices).
- usage of proven components.
- usage of open source components and frame works to have the code available.
- usage of standard industry interfaces.
- fully automated tests.
- implementation in well-known programming language.

The fulfilment of the standards and requirements shall be monitored and ensured continuously during the design and implementation process. Each deviation from the standards shall be justified. Before an agreement of deviation can be granted, an impact analyses must be undertaken. Agreed deviations are recorded. Versioning and traceability are preconditions for maintainability and are defined in the software architecture document.

### 3.1.4. SAC

Safety-related Application Conditions (SACs) as are bringing requirements to be fulfilled when interfacing safety related systems. SACs can imply high efforts regarding availability, maintainability and reliability of SubSys Plan Execution.

- The acknowledgement of these requirements shall be covered by the validation plan for SubSys Plan Execution.
- The fulfilment of the requirements shall explicitly be covered by the validation report for SubSys Plan Execution.

### 3.1.5. Safety

SubSys Plan Execution is envisaged as a non-safety-relevant system. It is not planned that SubSys Plan Execution assumes safety responsibility according to EN 50126-1 or EN 50128. No safety targets are expected and thus no risk-minimising measures are envisaged.

This determination is preliminary and will be reviewed in the further phases based on the results from the following documents.

- Validated risk analysis SubSys Plan Execution (EN 50126-1 phase 3 for SubSys Plan Execution).
- Released overall system RCA risk analysis (EN 50126-1 phase 3 for RCA).
- Released, final overall architecture RCA (EN 50126-1 phase 5 for RCA).
- Released, final assignment of safety requirements / safety functions to RCA SubSys based on the architecture (EN 50126-1 phase 5 for RCA).

The determination takes place in phase 3 with the risk analysis for SubSys Plan Execution. After the safety level has been defined, SubSys Plan Execution must fulfil the requirements according to the selected level.

As soon as the SACs (safety-relevant application rules according to EN 50128) of the systems with which interfaces exist are available, the assumptions regarding the interfaces are checked in the further phases. Without the SACs, for the existing interfaces explicitly requiring and permitting the transmission of safety-relevant data, SubSys Plan Execution may not assume any safety responsibility.

### 3.1.6. Security

The specifications on security are based on the consideration of the CIA protection goals. The CIA protection goals are Confidentiality, Integrity, Availability, Authenticity, Deniability, Reliability and Privacy.

The following definitions apply provisionally:

- **Confidentiality**: There are no special requirements for confidentiality. Neither special measures for the "protection of information behaviour" nor for the "protection of information content" are necessary.
- **Integrity**: The possibility of unauthorised data manipulation should be excluded. Unauthorised data manipulation can impair the availability and reliability of APS. Special requirements therefore exist

for integrity about the correctness of the data (data integrity) and regarding correct functioning of the system (system integrity).

- **Availability**: The requirements for availability can basically be found under 3.2 (Availability). From a security point of view, it must be considered that availability must not be reduced by attacks on the system.
- **Authenticity**: Special requirements exist about the proof of identity of all interface partners (partner authenticity) and the proof that the received data originate from the authenticated instance (data authenticity).
- **Deniability**: There are no specific requirements regarding deniability. Technical traceability of use (e.g. via data logging) must be given.
- **Reliability**: There are no specific requirements regarding reliability. Technical traceability of use (e.g. via data logging) must be given.
- **Privacy**: There are no special requirements regarding privacy. No communication processes need to be kept secret. Anonymous use of SubSys Plan Execution is not foreseen.

This determination is preliminary and will be reviewed based on the results from the following documents in the further phases.

- Released, final security requirements of the overall RCA system (EN 50126-1 phase 4 for RCA).
- Released, final overall architecture RCA (EN 50126-1 phase 5 for RCA).
- Released, final assignment of security requirements / security functions to RCA SubSys based on the architecture (EN 50126-1 phase 5 for RCA).

#### 3.1.7. RAMS Evaluation standards

*This section will be further elaborated in future releases*

## 3.2. RAMSS Policies and Targets from Railway Duty Holders

General note: The RAMSS policies and targets from railway duty holders will have to be analysed and defined country-specific.

## 3.3. Safety Legislation

#### 3.3.1.1. Safety Regulations

The development of SubSys Plan Execution takes place according to the recognised rules of technology. Recognised rules of technology manifest themselves in standards. EN 50128 is therefore applied to the development independently of the determination of the SIL; in the absence of a safety responsibility, further development takes place in SIL 0. EN 50128 applies to 'Railway applications - Telecommunications, signalling and data processing systems - Software for railway control and monitoring systems'. SubSys Plan Execution is a railway control and supervision system, non-application is generally not permitted.
Note: Further safety regulations will have to be analysed and defined country specific.

#### 3.3.1.2. Identified legislation and their impact

The following table lists the identified regulation with characteristic of relevant safety legislation for the SubSys Plan Execution incl. the impact on the system:

| Legislation | Impact on SubSys Plan Execution |
|---|---|
| Commission Implementing Regulation (EU) 2019/773 of 16 May 2019 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union and repealing Decision 2012/757/EU | Consideration of Interoperability |

| | |
|---|---|
| Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety | Consideration of Common safety methods ('CSMs')<br>In particular, consideration of Article 6 - Common safety methods ('CSMs'). |
| Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems | Implement specifications and processes according to EN 50128 |
| Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process | Observance of the processes according to EN 50126 - 1 |
| Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety | Observance of the processes according to EN 50126 - 2 |

Note: Further legislation aspects will have to be analysed and defined country-specific

## 3.4. Impacts from further Regulations

Note: Impacts from further regulations will have to be analysed and defined country-specific

## 3.5. Assumptions and Justifications

## 4. Issues

| Nr. | Title | Description |
|---|---|---|
| 1 | Add references to standards for RAMS evaluation and validation documents | Add one or more references to applied standards for RAMS evaluation and a list of necessary validation documents (deliverables). |
| 2 | RCA Posters | Integrate new version of RCA Posters and new SubSys Plan Execution interfaces as soon as description are given in Domain Knowledge. Complete document for consistency. |
| 3 | Objectives and System Requirements | Complete the chapter "Objectives and System Requirements" and finalise the derivation of the existing Objectives into System Requirements. |