RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

Concept: Plan Execution

Document id: RCA.Doc.47

Table of contents

List of Figures

List of Tables

Version History

Version	Date	Author	Description
0.1	2021-06-24	René Schönemann, Martin Kemkemer, Jens Wieczorek and other members of the RCA-OPE-Cluster	Preliminary version for RCA BL0 R2
0.2	2021-09-15	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	2021-11-30	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
0.4	2022-09-09	René Schönemann, Martin Kemkemer, Jens Wieczorek, Gabriele Löber, Rouzbeh Boloukian-Roudsari, Ulrich Schöni and Marcus Völcker as members of the RCA-OPE-Cluster	Release version for RCA BL1 R0

1. Introduction

1.1. Release information

Basic document information:

RCA-Document Number: 47

Document Name: Concept: Plan Execution

Cenelec Phase: 1

Version: 0.4

RCA Baseline set: BL1R0

Approval date: 2022-09-30

1.2. 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.

1.3. 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.

1.4. Purpose of the document

This document is the system concept of SubSys Plan Execution (PE). It describes the system context of SubSys Plan Execution and derives its system requirements from the objectives defined in A.P.M. Objectives [RCA.Doc.53]. The concept also contains the envisaged RAMS requirements of SubSys Plan Execution.

1.5. 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.*

1.6. Structure of Document

This concept is structured as follows:

- Chapter 1 gives a short introduction to the document
- Chapter 2 describes the scope, context and environment of SubSys Plan Execution
- Chapter 3 lists the objectives defined for SubSys Plan Execution and the system requirements derived from them
- Chapter 4 contains the envisaged RAMSS requirements for SubSys Plan Execution
- Chapter 5 lists issues which will be addressed in future releases of this concept

1.7. Related documents

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

- RCA System Architecture [RCA.Doc.35]
- RCA Terms and Abstract Concepts [RCA.Doc.14]
- A.P.M. Business strategy, targets and problem definition [RCA.Doc.50]
- A.P.M. Objectives [RCA.Doc.53]
- Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]

- Concept: Architectural Design for Plan Execution [RCA.Doc.49]
- RCA Architecture Poster [RCA.Doc.40]
- RCA Position paper: Comparison and matching proposal of APS-SM (RCA) and IPM-ERM (DBS) [RCA.Doc.75]
- Solution Concept MAP [RCA.Doc.54]

2. System

The SubSys Plan Execution is a connecting SubSys between the Planning System (PAS) and SubSys Safety Logic (see Figure 1).

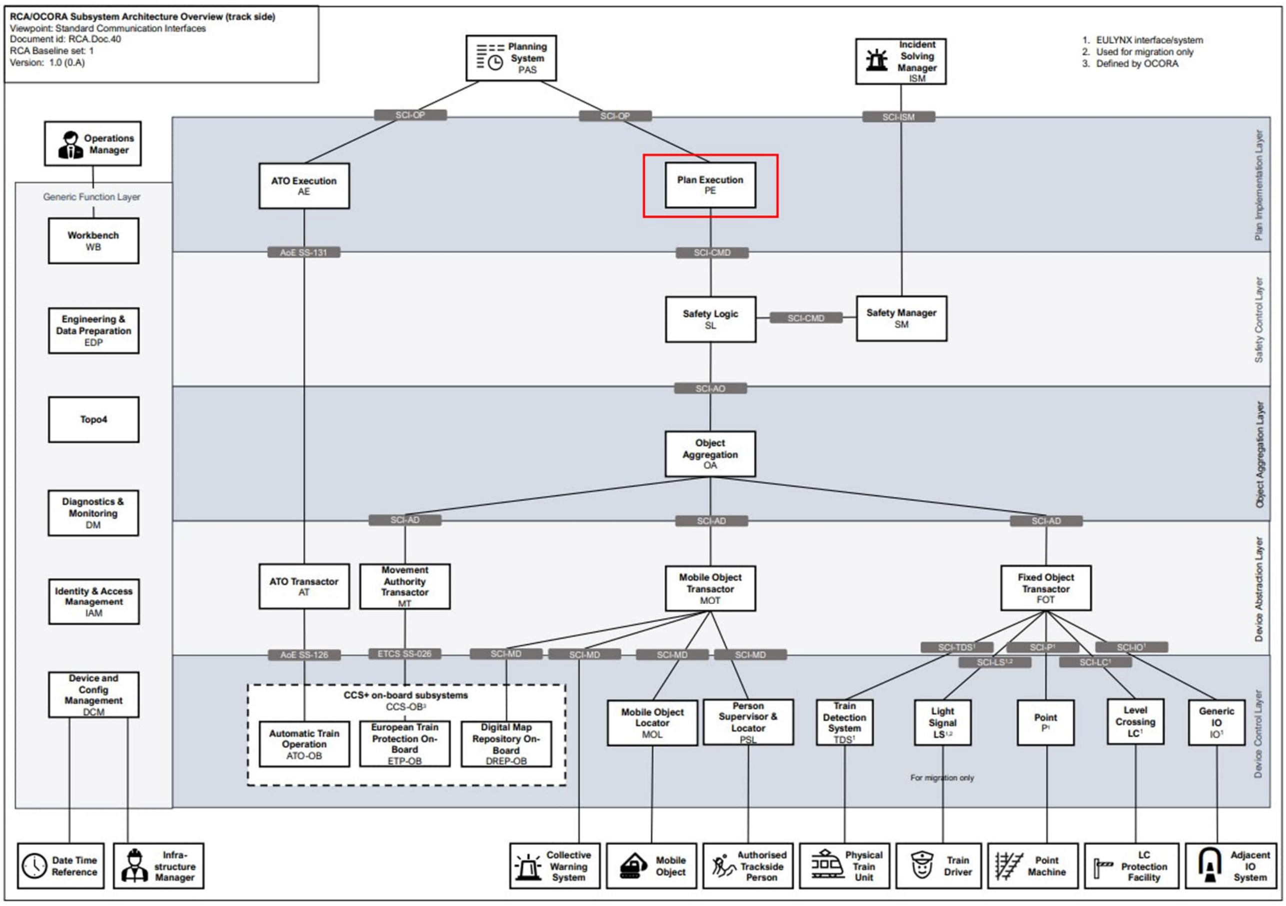

Figure 1: SubSys Plan Execution within Railway System as defined by RCA [RCA.Doc.40]

The Planning System (PAS) manages the optimal capacity utilisation of the railway infrastructure in the AoC. The Planning System (PAS) continuously re-plans the timetable and decides about measures to optimise the flow of traffic on the network. PAS is typically a large IT system landscape which delivers a production plan. The production plan formed by the PAS is analysed and executed by “plan execution” control systems. The subsystem Plan execution (PE) forms the discrete requests for securing the Track Path and sends them to the Safety Logic SL.

2.1. Scope

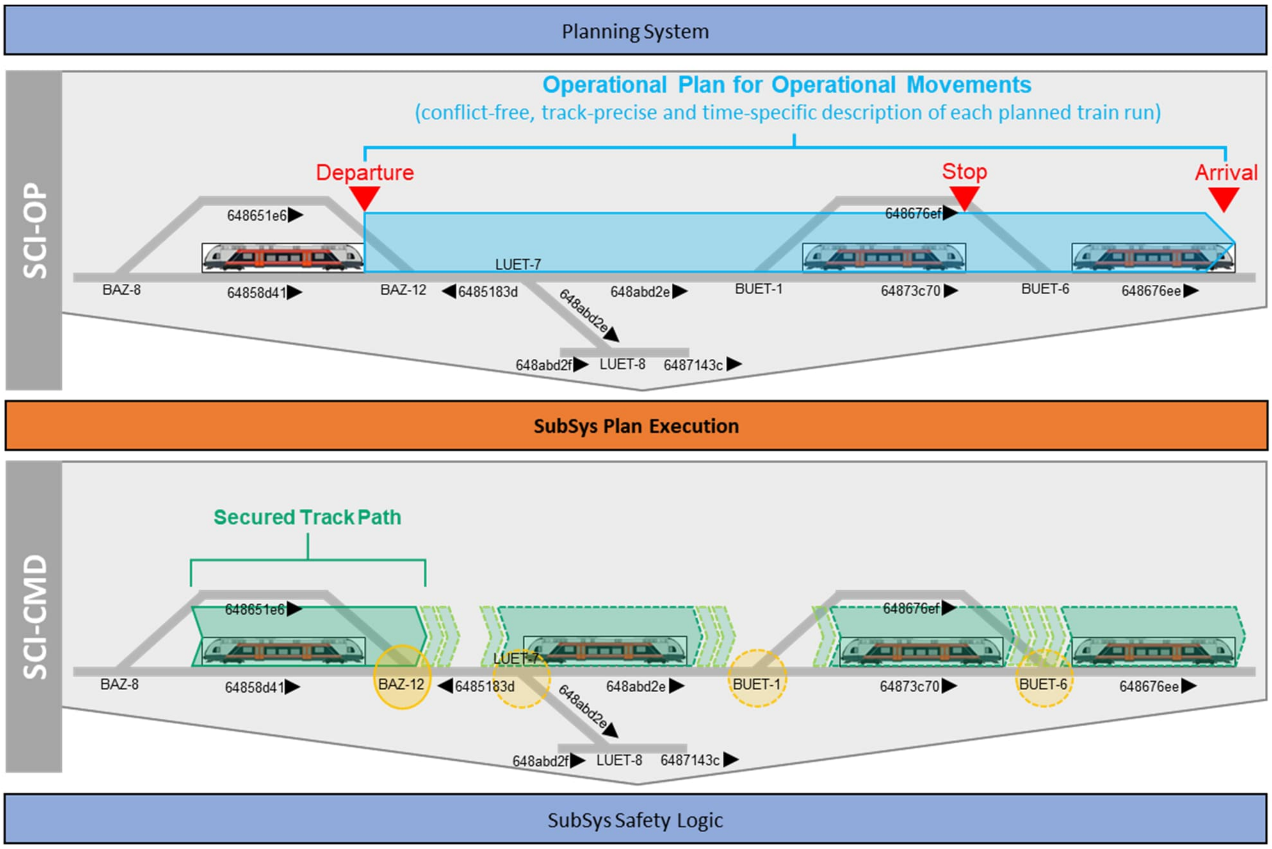

Figure 2: Illustration of SubSys Plan Execution and the two interfaces SCI-OP and SCI-CMD

SubSys Plan Execution is a railway control and monitoring system. The core functionality of SubSys Plan Execution is the automatic and precise execution of the Operational Plans sent by the external Planning System (PAS), see Figure 2.

- 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 as Usage Restriction Area and Warning Areas from SubSys Safety Logic.
- SubSys Plan Execution considers the dependencies between different Operational Plans as specified by the Planning System.

All of this core functionality is based on the knowledge of the APS Operating State, a safe logical representation of the actual state of railway operations in the Area of Control. Via the Standard Communication Interface - Command (SCI-CMD), the SubSys Safety Logic provides the APS Operating State. The APS Operating State is then processed by SubSys Plan Execution and extended with additional information not known by APS (references to Operational Plans, Operational Usage Restrictions, etc.). Afterwards, SubSys Plan Execution provides the PE Operating State with the additional information via the Standard Communication Interface - Operational Plan (SCI-OP) to the Planning System outside the system border of RCA.
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 SubSys Safety Logic.
Characteristics of SubSys Plan Execution:

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

- works without knowledge of business rules (e.g. Timetable Rules, Capacity Planning) which are handled by the Planning System (PAS) and 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)

2.1.1. Features

- Precise implementation of Operational Plans for Operational Movement, Operational Restriction and Operational Warning Measure sent by the Planning System.
    - Requests the required 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 (create, update, delete) by deriving required Usage Restriction Areas and sending requests to SubSys Safety Logic at the specified time.
    - Implement Operational Warning Areas (create, update, delete) by sending requests to SubSys Safety Logic at the specified time.
    - 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 APS Operating State and provide this information to the Planning System in near real time.
- Provide information and commands needed for manual operation of SubSys Plan Execution via SubSys Workbench (temporary fallback level for the Planning System, unplanned manual interactions, use of existing CTC systems if no PAS is available during migration).

SubSys Plan Execution is characterized by very high availability, very low latency and very short and deterministic reaction times.

2.1.2. Overview of functionality

SubSys Plan Execution provides the following functionality:

- **Operational Plan management**
    - Function: Process Operational Plan

- **Automatic plan execution**
    - **Driveability management**
        - Function: Observe driveability of railway network
          Note: This is done by processing the APS Operating State received via SCI-CMD

        - Function: Provide driveability of railway network
          Note: This is done by providing information about driveability of railway network as part of the PE Operating State via SCI-OP and SWI-PE

        - Function: Control driveability of railway network
          Note: This is done by sending the required commands to SubSys SL via SCI-CMD
            - Subfunction: Calculate Trigger Points for driveability requests

    - **Operational Movement management**
        - Function: Observe Operational Movement of Physical Train Units
          Note: This is done by processing the APS Operating State received via SCI-CMD

        - Function: Provide Operational Movement of Physical Train Units
          Note: This is done by providing information about Operational Movement of Physical

Train Units as part of the PE Operating State via SCI-OP and SWI-PE

    - Function: Control Operational Movement of Physical Train Units
      Note: This is done by sending the required commands to SubSys SL via SCI-CMD
        - Subfunction: Calculate MP
            - Subfunction: Calculate MP Extent
            - Subfunction: Calculate Risk Buffer
            - Subfunction: Calculate Risk Paths
        - Subfunction: Calculate Trigger Points for MP requests

  - **Operational Restriction management**
    - Function: Observe Usage Restriction Areas on railway network
      Note: This is done by processing the APS Operating State received via SCI-CMD

    - Function: Provide Operational Restriction Areas on railway network
      Note: This is done by providing information about Operational Restriction Areas on railway network as part of the PE Operating State via SCI-OP and SWI-PE

    - Function: Control Operational Restriction Areas on railway network
      Note: This is done by sending the required commands to SubSys SL via SCI-CMD
        - Subfunction: Define safeguard measures (Usage Restriction Areas)

  - **Operational Warning Measure management**
    - Function: Observe Warning Areas on railway network
      Note: This is done by processing the APS Operating State received via SCI-CMD

    - Function: Provide Operational Warning Areas on railway network
      Note: This is done by providing information about Operational Warning Areas on railway network as part of the PE Operating State via SCI-OP and SWI-PE

    - Function: Control Operational Warning Areas on railway network
      Note: This is done by sending the required commands to SubSys SL via SCI-CMD

- **Manual operation (via Workbench)**
  - Function: Manual plan execution
  - Function: Manual control of field elements

- **Device and Configuration Management**
  - Function: Import Configuration Data
  - Function: Activate Map Data

- **Monitoring and Diagnostics**
  - Function: Send diagnostics data

Besides the functionality listed above, SubSys Plan Execution provides the following functions to implement RAMSS requirements:

  - Function: Use authentication and authorisation services
  - 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 integrity and check internal data model
  - Function: Synchronise the state of Configuration Data and Operational Data

2.2. Out of scope

The functions listed below are not part of the scope of SubSys Plan Execution, although they are included in current systems such as existing centralised 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 Plans 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 (catenary equipment, axle load compatibility, etc.) 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

- Obviously, 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 work according to 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.
- **Railway network 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 Movement 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. According to the required safety level, the tracking and processing of such vehicles, personal and devices will be in the

    responsible of the APS Safety Manager (APS-SM) or in the responsibility of the Evaluation Reaction Manager (IPM-ERM), see [RCA.Doc.75].
  - SubSys Plan Execution is not responsible for matching warning devices to Operational Warning Areas or setting up warning devices
  - SubSys Plan Execution does not activate or de-activate warning devices to warn Physical Train Units, non-track-bound vehicles or trackside persons within or close to a warning area (SubSys Plan Execution does only create, update and delete warning areas).

Alarms regarding hazardous situations

- SubSys PE does not process alarms regarding hazardous situations (e.g avalanche sensors, hot box detector, short circuit in catenary sections, emergency call of driver, etc).

2.3. Context

2.3.1. RCA

The context of SubSys Plan Execution within RCA (see Figure 1) is defined as follow:

- SubSys Plan Execution is defined in the RCA. In terms of the overall RCA, it is a SubSys.
- SubSys Plan Execution is defined as a product.
- SubSys Plan Execution is currently envisaged as a non-safety-relevant system.
- The development process should nevertheless be done according to EN 50126-1 and EN 50128, as one must develop according to these standards from Basic Integrity. The actual safety 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 its interfaces the compliance with international standards (e.g. TSI TAF/TAP, RailML) is 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 system, thus achieving scalability).
- SubSys Plan Execution has an interface (SHI-PE) to other neighbouring SubSys Plan Execution to work in a joint network (as an example, via this interface parts of the PE Operating State can be exchanged with a neighbouring SubSys Plan Execution instance).

2.3.2. 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.

2.3.3. 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).

2.4. Environment

2.4.1. Physical influences

The technical system, SubSys Plan Execution, is executed on a computing platform containing hardware as well as software (board support package, operating systems, runtime environment, etc.). It will be in the responsibility of the computing platform to deal with physical influences.

Note: For further information about the computing platform, see "White paper: An Approach for a Generic Safe Computing Platform for Railway Applications" [TWS03-10].

2.4.2. 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 briefly the interfaces from and to SubSys Plan Execution.

2.4.2.1. SCI-OP

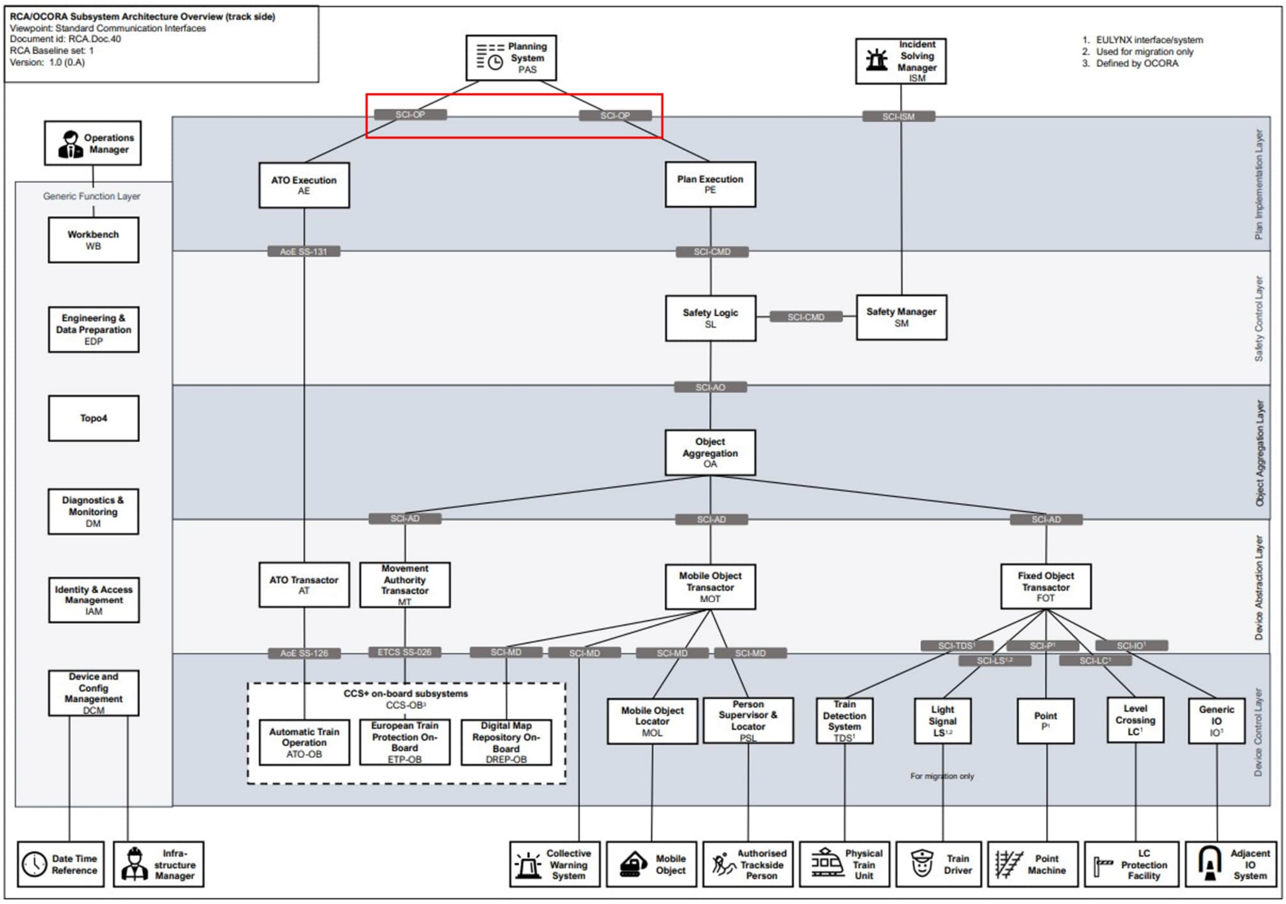

Figure 3: SCI-OP in the RCA Logical Architecture [RCA.Doc.40]

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.
- **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 PE and AE Operating State (entities: Train Unit Report, Track Allocation, Operational Restriction Area, Operational Warning Area, Field Element State)

Please refer to Concept SCI-OP [RCA.Doc.31] for details about this interface.

2.4.2.2. SCI-CMD

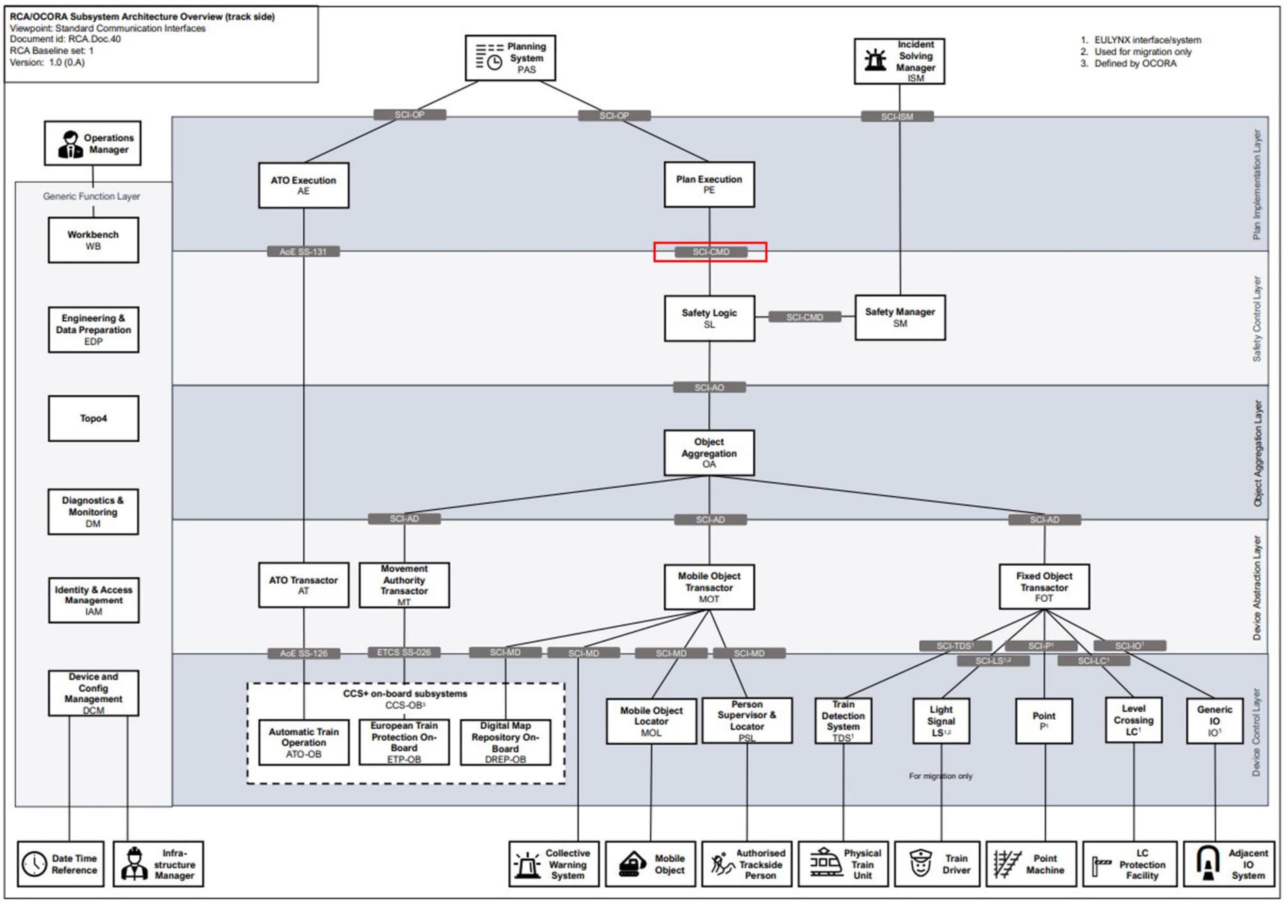

Figure 4: SCI-CMD in the RCA Logical Architecture [RCA.Doc.40]

Description of SCI-CMD

Please refer to Concept SCI-CMD [RCA.Doc.70] for details about this interface.

2.4.2.3. SWI-PE

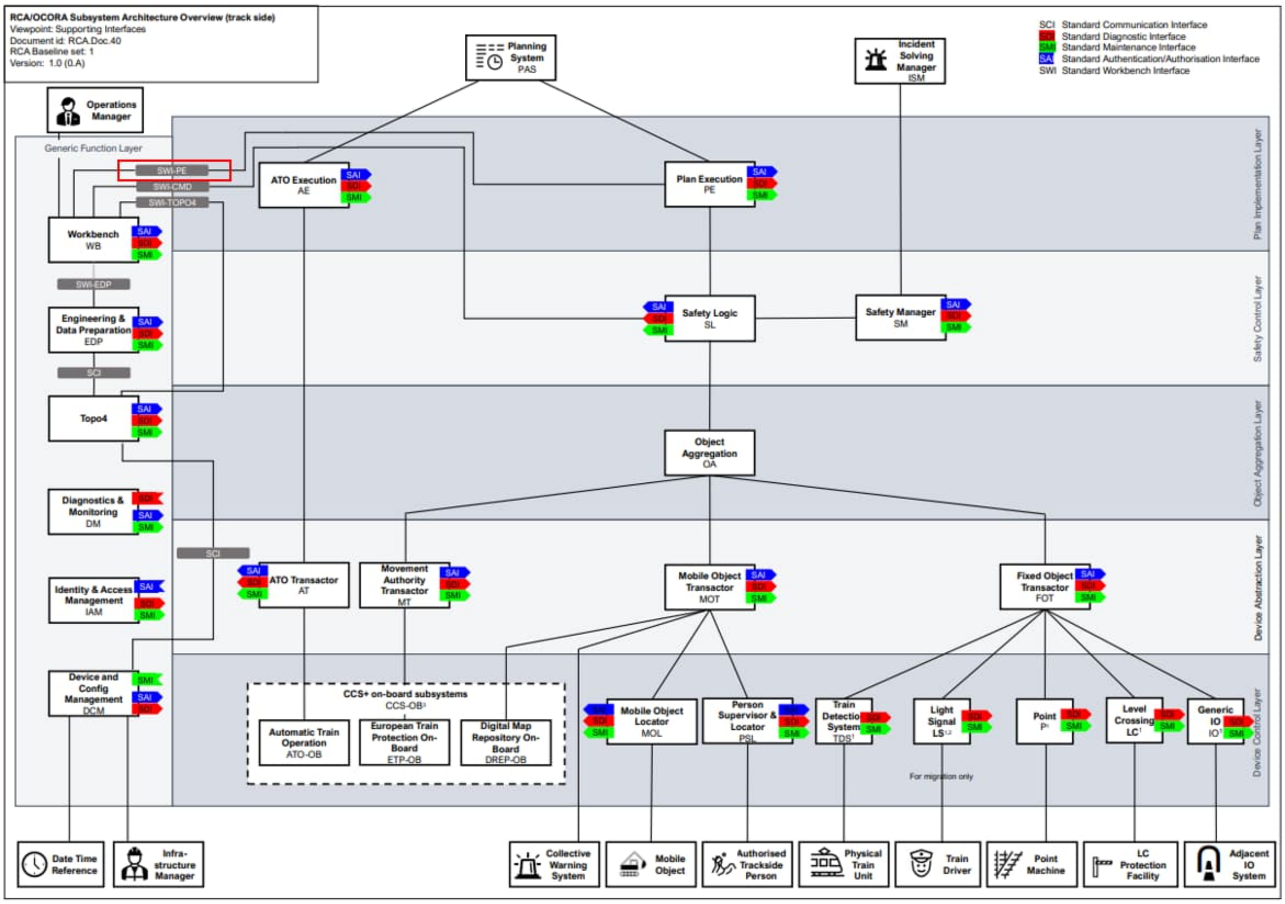

Figure 5: SWI-PE in the RCA Logical Architecture [RCA.Doc.40]

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 transparently to the application layer. The latter shall provide the user interaction for the Authorised 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 manual control of field elements
- **Upstream:**
  - Provide Operational Plan Execution (entities: Operational Plan Execution Response, Operational Plan Execution Report, Operational Plan Execution Forecast)
  - Provide PE Operating State (entities: Train Unit Report, Track Allocation, Operational Restriction Area, Operational Warning Area, Field Element State)

Note:

There is not yet a concept document which describes the SWI-PE interface in more detail. Please refer to RCA System Architecture [RCA.Doc.35] for more information.

2.4.2.4. SHI-PE

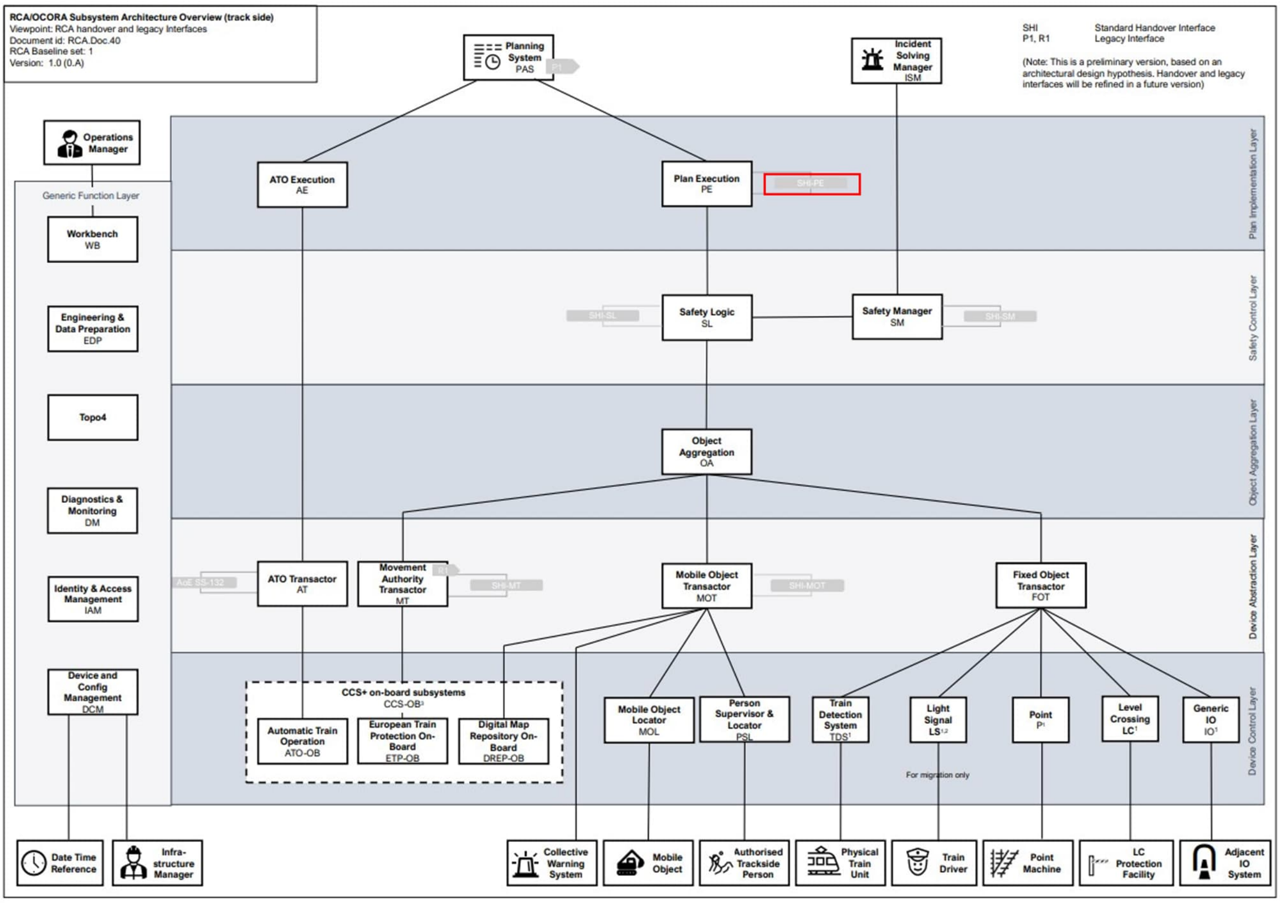

Figure 6: SHI-PE in the RCA Logical Architecture [RCA.Doc.40]

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 (e.g. parts of the PE Operating State) and to pass a Physical Train Unit from one Area of Control to the next.

Note:

There is not yet a concept document which describes the SHI-PE interface in more detail. Please refer to RCA System Architecture [RCA.Doc.35] for more information.

2.4.3. Cross sectional system interfaces

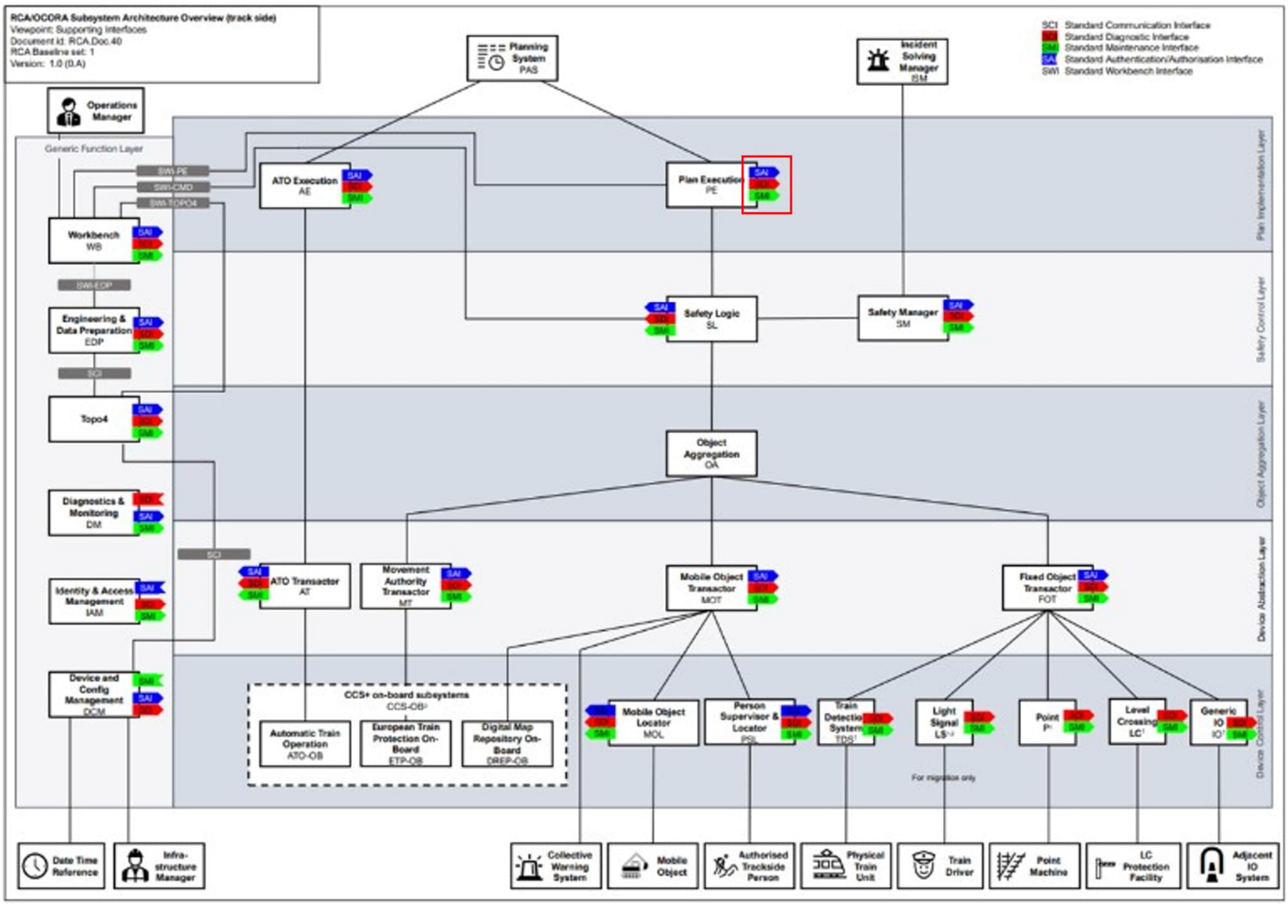

Figure 7: SMI, SDI, SAI in the RCA Logical Architecture [RCA.Doc.40]

2.4.3.1. SMI

Description of SMI

The interface SMI is described in detail in document Concept SMI [RCA.Doc.74].

2.4.3.2. SDI

Description of SDI

There is not yet a concept document which describes the SDI interface in more detail. Please refer to RCA System Architecture [RCA.Doc.35] for more information. SAI

2.4.3.3. SAI

Description of SAI

There is not yet a concept document which describes the SAI interface in more detail. Please refer to RCA System Architecture [RCA.Doc.35] for more information. Legal aspects

2.4.4. Legal aspects concern:

1. Occupational safety e.g. for usability graphical user interfaces
2. Functional 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 4.3.

3. Objectives and System Requirements

The tables in the following subchapters list:

- the objectives for SubSys Plan Execution defined in A.P.M. Objectives [RCA.Doc.53] (column “Objective PE” resp. column “Objective A.P.M”)
- the system requirements for Plan Execution derived from these objectives (column “System Requirement”)
- a reference to the concept which further refines the system requirements (column “Reference to Concept”)

Figure 8 gives an overview of the different documents and their relationship to each other.

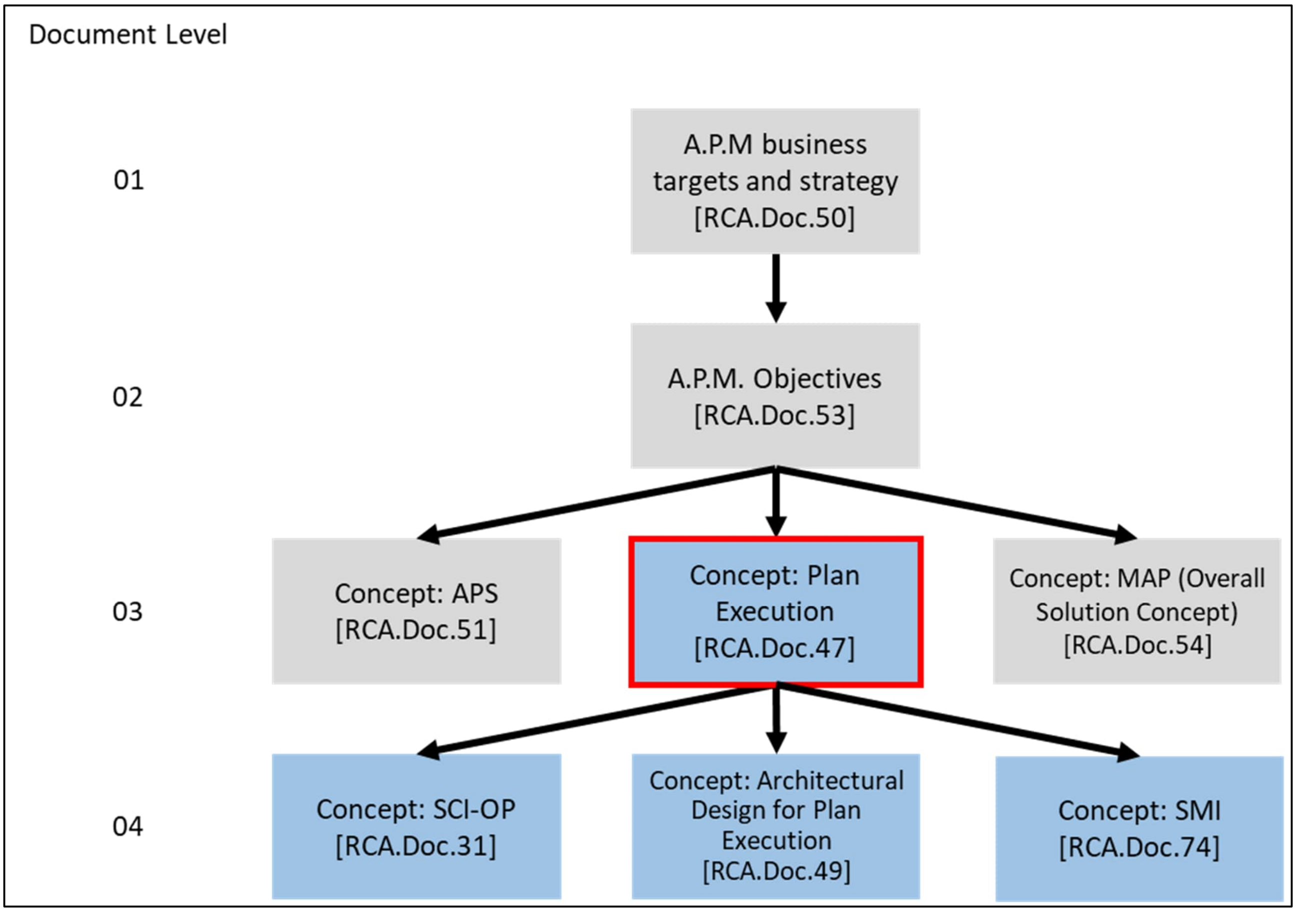

Figure 8: Document Relations

This section will be further elaborated in future releases

3.1. Category: Plan Execution

Table 1: Plan Execution Objectives and Systems Requirements PE

Objective PE	System Requirement	Reference to Concept
O-PE@Ensure the precise implementation of Operational Plans for Operational Movements, Operational Restrictions and Operational Warning Measures (fully automated) O-PE@Execute Operational Plans considering the operationally needed safety level and the possible risk mitigation measures	• SubSys Plan Execution shall ensure the precise 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 APS Operating State • SubSys Plan Execution shall constantly monitor the current APS Operating State • SubSys Plan Execution shall implement the Operational Plans to the earliest point in time possible, but it shall request	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: Calculation of MP and triggering of requests via SCI-CMD

<table>
<tr><td>O-PE@Execute Operational Plans by requesting Movement Permissions with any operationally appropriate geometric extension.</td><td rowspan="5">Movement Permissions and Field Element States only, if immediate needed, so that the Planning System is able the perform a replanning if needed.
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 precise implementation of Operational Plans
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
SubSys Plan Execution shall enable the closest possible sequence of train movements
SubSys Plan Execution shall ensure that trains can run continuously without unscheduled stops</td><td rowspan="5"></td></tr>
<tr><td>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</td></tr>
<tr><td>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.</td></tr>
<tr><td>O-PE@Request the driveability and flank protection state of Field Elements of the railway network to execute Operational Movements</td></tr>
<tr><td>O-PE@Request Movement Permissions for Physical Train Units to execute Operational Movements</td></tr>
<tr><td rowspan="3">O-PE@Provide information required for the operation of the RCA system</td><td>SubSys Plan Execution shall execute Operational Plan requested via SCI-OP
SubSys Plan Execution shall provide the PE Operating State via SCI-OP
SubSys Plan Execution shall provide the Execution State of Operational Plans via SCI-OP
SubSys Plan Execution shall provide the PE Operating State via SWI-PE
SubSys Plan Execution shall provide the Execution State of Operational Plans via SWI-PE
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</td><td>Concept: Architectural Design for Plan Execution [RCA.Doc.49]

Functional concept: TBD</td></tr>
<tr><td>SCI-OP shall allow requesting the execution of Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings
SCI-OP shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings
SCI-OP shall allow requesting the departure, arrival, or passage times of an Operational Movement
SCI-OP shall allow requesting the execution order of different Operational Movements
SCI-OP shall provide the PE and AE Operating State
SCI-OP shall provide the Execution State of Operational Plans
SCI-OP shall provide the Execution Forecast of Operational Plans
SCI-OP shall provide information in such a granularity and format that it is suitable for RCA external target systems consuming the information correct and efficient</td><td>Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]</td></tr>
<tr><td>SWI-PE shall allow to request the execution of Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings
SWI-PE shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings
SWI-PE shall allow to request the departure, arrival, or passage times of an Operational Movement
SWI-PE shall allow to request the execution order of different Operational Movements
SWI-PE shall allow to provide the PE Operating State
SWI-PE shall allow to provide Execution State of Operational Plans</td><td>Concept: TBD</td></tr>
</table>

	• SWI-PE shall allow to provide information in such a granularity and format that it is suitable for SubSys WB	
O-PE@Receive and process initial and update requests for Operational Plans	• SubSys Plan Execution shall be able to receive and process initial requests for Operational Plans • SubSys Plan Execution shall be able to receive and process update requests for Operational Plans • SubSys Plan Execution shall always know the latest version of an Operational Plan	Concept: Architectural Design for Plan Execution [RCA.Doc.49] 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] 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: 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] Functional concept: TBD
	• SCI-OP shall allow requesting automated coupling and decoupling of Physical Train Units	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
	• SWI-PE shall allow requesting automated coupling and decoupling of Physical Train Units	Concept: 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] Functional concept: TBD

3.2. Category: Robustness

Table 2: Robustness Objectives and Systems Requirements PE

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. • 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. • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with failures of Field Elements • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with degraded modes of Field Elements • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with temporary restrictions of the railway network • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with Track Allocations of the railway network • SubSys Plan Execution shall implement retry mechanisms for unsuccessfully executed Operational Events (e.g. in case of stucked Field Elements) • 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] 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. • 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 • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with failures of Physical Train Units • SubSys Plan Execution shall request Movement Permission with specific characteristics to cope with degraded modes of Physical Train Units • SubSys Plan Execution shall support the handling of identified, but not safely localized Physical Train Units • SubSys Plan Execution shall support the handling of unidentified but localized Physical Train Units • 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] 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. • 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] Functional concept: System States, Operational States and Modes of Operation
	• SubSys Plan Execution shall be able to check the integrity of its internal data model • 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] Functional concept: Robustness and High availability
	• SDI shall allow to receive the System State and Operational State of the Planning System	Concept: 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. • 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] Functional concept: System States, Operational States and Modes of Operation
	• SubSys Plan Execution shall be able to check the integrity of its internal data model • 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] Functional concept: Robustness and High availability
	• SDI shall allow to receive the System State and Operational State of other RCA SubSys	Concept: 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 • SubSys Plan Execution shall be able to provide its System State and Operational State to other RCA SubSys	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: System States, Operational

	• SubSys Plan Execution shall be able to provide its System State and Operational State to the Planning System • SubSys Plan Execution shall retry to use its capabilities as soon as they are available again.	States and Modes of Operation
	• SubSys Plan Execution shall be able to check the integrity of its internal data model. • 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] Functional concept: Robustness and High availability
	• SDI shall allow to provide the internal System State and Operational State to other RCA SubSys	Concept: 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. Note: The current working hypothesis is that SubSys Plan Execution is Basic Integrity or has No SIL at all. If this hypothesis is confirmed by the detailed risk analysis, this requirement will be changed.	Concept: Architectural Design for Plan Execution [RCA.Doc.49] 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 • SubSys Plan Execution shall support availability through redundant system instances and hot standby mechanisms • SubSys Plan Execution shall be able to check the integrity of its internal data model • 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 • 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] Functional concept: TBD
	• SWI-PE shall support manual operation of RCA by SubSys WB	Concept: TBD

Table 3: Robustness Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Handle internal failures and degraded modes 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. • 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] Functional concept: System States, Operational States and Modes of Operation

	• SubSys Plan Execution shall be able to check the integrity of its internal data model • 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] Functional concept: Robustness and High availability
	• SDI shall allow to receive the System State and Operational State of the Planning System	Concept: 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
A.P.M.@Malfunctioning of system components shall not lead to a shutdown of the system	• SubSys Plan Execution shall be able to work at least in degraded mode if other RCA SubSys are malfunctioning or not available • SubSys Plan Execution shall be able to work at least in degraded mode if internal subsystems are malfunctioning	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional 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	• 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	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: System States, Operational States and Modes of Operation
A.P.M.@The overall system should be as robust as possible against version changes and missing information	• SubSys Plan Execution shall provide generic capability-based interfaces	Concept: TBD
A.P.M.@Support of self/remote diagnostics	• 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 • SubSys Plan Execution shall be able to check the integrity of its internal data model	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: System States, Operational States and Modes of Operation
	• SubSys Plan Execution shall monitor the processing of its functions by collecting information about the processing states and results (based on the definition of RAMSS related parameters) • SubSys Plan Execution shall store the monitoring and diagnostic data for later reports and analysis.	Concept: TBD
	• SDI shall allow to receive the System State and Operational State of other RCA SubSys • SDI shall support the delivery of diagnostics data from RCA SubSys	Concept: TBD

3.3. Category: Migration Strategy

Table 4: Migration Objectives and Systems Requirements PE

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 completely or partially are located within its Area of Control • SubSys Plan Execution shall ensure the efficient handover of Operational Movements from and to adjacent SubSys Plan Execution via SHI-PE	Concept: TBD
O-PE@Support migration for existing CTC Systems	• SubSys Plan Execution shall ensure the efficient handover of Operational Movements from and to adjacent legacy CTC Systems	Concept: TBD

	• SCI-OP shall support dedicated migration options by supporting existing CTC Systems. • SCI-OP shall be independent from operational processes • SCI-OP shall support different kinds and granularities of Operational Plans independent from provided functionality and behaviour of the Physical Train Units and Field Elements	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
	• SWI-PE shall support dedicated migration options by supporting existing CTC Systems Note: See “Concept: Architectural Design for Plan Execution [RCA.Doc.49]” for a rational for this requirement.	Concept: TBD
O-PE@Support migration for different expansion stages of Planning Systems	• SubSys Plan Execution shall implement functionality to support different expansion stages of Planning Systems	Concept: TBD
	• 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 • SubSys Plan Execution shall provide the functionality to operate APS based on information sent and received via SWI-PE by SubSys WB • 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] Functional concept: TBD
O-PE@Guarantee railway operation with a mixed ETCS level approach (L2/L3) of trains and railway network	• SubSys Plan Execution shall guarantee railway operation with a mixed ETCS level approach (L2/L3) of trains and railway network	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
O-PE@Support different ATO levels (GoA1 – GoA4) and ETCS levels (L2/L3) and a mixed level approach	• SCI-OP shall support different ATO levels (GoA1 – GoA4) and ETCS levels (L2/L3) and a mixed level approach	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
	• SubSys Plan Execution shall guarantee railway operation with a mixed ETCS level approach (L2/L3) of trains and railway network	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
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 (e.g. min/max extend of MP)	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
	• SMI shall be able to provide national specific operating rules (e.g. min/max extend of MP)	Concept: Standard Maintenance Interface [RCA.Doc.74]
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 handover of Operational Movements from and to adjacent legacy CTC Systems	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
	• SHI-PE shall support the handover of Operational Movements from and to adjacent legacy CTC Systems	Concept: 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

Table 5: Migration Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Allow different system layouts from decentralised to highly centralised safe computing with virtualization and container technologies, n-modular redundancy, fast disaster recovery, multi-tenant and multi-company cloud structures	• 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 Note: The current working hypothesis is that SubSys Plan Execution is Basic Integrity or has No SIL at all. If this hypothesis is confirmed by the detailed risk analysis, this requirement will be changed. • SubSys Plan Execution shall have a strong separation of SW and HW concerns	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)	• SubSys Plan Execution shall ensure the efficient handover of Operational Movements from and to adjacent legacy CTC Systems • SubSys Plan Execution shall implement functionality to support different expansion stages of Planning Systems	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
	• SCI-OP shall support dedicated migration options by supporting existing CTC Systems • SCI-OP shall be independent from operational processes • SCI-OP shall support different kinds and granularities of Operational Plans independent from provided functionality and behaviour of the Physical Train Units and Field Elements • SCI-OP shall support different expansion stages of Planning Systems	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
	• SWI-PE shall support dedicated migration options by supporting existing CTC Systems	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
A.P.M.@Provide scalable system architecture to be used in a modular way depending on local needs	• SubSys Plan Execution shall work independently of the functionality of neighbouring SubSys, therefore no assumptions about dedicated behaviour shall be made	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
	• SCI-OP shall be independent from operational processes • SCI-OP shall support different kinds and granularities of Operational Plans independent from provided functionality and behaviour of the Physical Train Units and Field Elements	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]

3.4. Category: RAM Strategy

Table 6: RAM Objectives and Systems Requirements PE

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 Note: The current working hypothesis is that SubSys Plan Execution is Basic Integrity or has No SIL at all. If this hypothesis is confirmed by the detailed risk analysis, this requirement will be changed to RAM requirements only.	Concept: TBD

Table 7: RAM Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Architecture design reduces the functional and non-functional dependencies between the	• SubSys Plan Execution shall achieve No SIL or Basic Integrity per function • SubSys Plan Execution shall be highly available	Concept: TBD

SubSys and thus reduces the functional and non-functional requirements (especially RAMS) for the individual SubSys.		
A.P.M.@Demonstrably successful best practices in software development for highly available systems should be applied	• SubSys Plan Execution shall be developed according to EN 50128 and EN 50126-1	Concept: TBD
A.P.M.@Provide data about system behaviour about RAMS and capacity usage to other systems	• SubSys Plan Execution shall monitor the processing of its functions by collecting information about the processing states and results (based on the definition of RAMSS related parameters) • SubSys Plan Execution shall store the monitoring and diagnostic data for later reports and analysis.	Concept: TBD
	• SDI shall support the delivery of diagnostics data from RCA SubSys	Concept: TBD
A.P.M.@Reduce maintenance efforts by maximally reducing dependencies between building blocks	• SubSys Plan Execution shall work independently of the functionality of neighbouring SubSys, therefore no assumptions about dedicated behaviour shall be made	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD

3.5. Category: Safety Strategy

Table 8: Safety Objectives and Systems Requirements PE

Objectives PE	System Requirements	Reference to Concept
O-PE@Develop RCA SubSys according to EN 50128 and EN 50126	• SubSys Plan Execution shall be developed according to EN 50128 and EN 50126-1	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	• SWI-PE shall provide information required to implement specific unscheduled manual operations which require up to SIL 2 in SubSys WB Note: The current working hypothesis is that SubSys Plan Execution is Basic Integrity or has No SIL at all. Therefore, this objective is derived to SWI-PE only	Concept: TBD

Table 9: Safety Objectives and Systems Requirements A.P.M.

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	• SubSys Plan Execution shall achieve No SIL or Basic Integrity per function.	Concept: TBD
A.P.M.@Design a modular system architecture with small as possible amount of safety relevant components	• SubSys Plan Execution shall achieve No SIL or Basic Integrity	Concept: TBD

3.6. Category: Security Strategy

Table 10: Security Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept

A.P.M.@Avoid unnecessary authorisation by building trusted clusters	• SubSys Plan Execution shall use a central identity, access and key management provided via SAI	Concept: TBD
A.P.M.@Ensure security by design for all SubSys and data flows according to RCA	• SubSys Plan Execution shall be developed according to a Secure Development Lifecycle (SDL) process as defined in TS 50701 / IEC 62443-4-1	Concept: TBD
A.P.M.@Support the integration with state of the art identity and access management service	• SubSys Plan Execution shall use a central identity, access and key management provided via SAI	Concept: TBD

3.7. Category: Life Cycle Management and Updateability

Table 11: Life Cycle Management and Updateability Objectives and Systems Requirements PE

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. • SubSys Plan Execution shall 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

Table 12: Life Cycle Management and Updateability Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Asset management must support the demand for high-cadence asset modification	• SubSys Plan Execution shall 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
	• SubSys Plan Execution shall be able to be operated during a Map Data Version Update • SubSys Plan Execution shall ensure that the Map Data Version Update is accomplished in the shortest possible time to minimize the unavailability of updated Map Data Elements	Solution Concept MAP [RCA.Doc.54] Solution Concept MAP – PUB-TS phase
	• SubSys Plan Execution shall be able to receive, and process update requests for Operational Plans	Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: Requesting of Operational Plans
	• SCI-OP shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
	• SWI-PE shall allow updates of already requested Operational Plans for Operational Movements, Operational Restrictions and Operational Warnings	Concept: TBD
A.P.M.@Build a modular system architecture that supports different lifecycles	• SubSys Plan Execution shall have a strong separation of SW and HW concerns	Concept: TBD

	• SubSys Plan Execution functions shall be grouped into SubSys Plan Execution internal building blocks according to their lifecycle.	
A.P.M.@Enable changes, adaptations and extensions throughout the life cycle of the building blocks	• SubSys Plan Execution shall provide generic capability-based interfaces	Concept: TBD
A.P.M.@Exchangeability between building blocks must be present wherever non-overlapping technology lifecycle profiles are present	• SubSys Plan Execution shall provide generic capability-based interfaces • SubSys Plan Execution shall have a strong separation of SW and HW concerns	Concept: TBD
A.P.M.@Overlapping technology lifecycle profiles must be respected by the system design	• SubSys Plan Execution functions shall be grouped into SubSys Plan Execution internal building blocks according to their lifecycle.	Concept: TBD
A.P.M.@Build a modular system architecture that is split according to different lifecycles	• SubSys Plan Execution functions shall be grouped into SubSys Plan Execution internal building blocks according to their lifecycle.	Concept: TBD
A.P.M.@Support fast module replacement	• SubSys Plan Execution shall have a strong separation of SW and HW concerns • SubSys Plan Execution shall have generic application logic that works independently of the content of the Map Data, if the structure of the Map Data is respected • SubSys Plan Execution shall provide generic capability-based interfaces	Concept: TBD

3.8. Category: Standardisation, Automation, and Integration

Table 13: Standardisation, Automation, and Integration Objectives and Systems Requirements PE

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 • SubSys Plan Execution shall ensure that the Map Data Version Update is accomplished in the shortest possible time to minimize the unavailability of updated Map Data Elements.	Solution Concept MAP [RCA.Doc.54] Solution Concept MAP – PUB-TS phase Capability: Activate Map Data Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
O-PE@Process (partly automated) alarms regarding hazardous situations (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] 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 • SubSys Plan Execution shall support easy adaptable interface for avoiding manual data exchange efforts • 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] Functional concept: TBD

	• SDI shall support the provisioning of diagnostics data from RCA SubSys	Concept: 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

Table 14: Standardisation, Automation, and Integration Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Accompanying standardisation to reduce system compatibility testing between onboard and trackside	• SubSys Plan Execution shall have no dependencies to technical details of Physical Train Unit	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	• SubSys Plan Execution shall support MAP data activation • SubSys Plan Execution shall be able to forward the MAP Data Activation Time to SubSys DCM	Concept: TBD
	• SCI-OP shall support transmission of MAP Data Activation Time	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
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	• SubSys Plan Execution shall be able to operate as a single active in-stance for an entire geographical segment which includes today multiple interlockings	Concept: TBD
A.P.M.@Consider open interfaces to integrate as much formats as possible	• 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 • All SubSys Plan Execution specifications shall be freely available to anybody at no cost	Concept: TBD
A.P.M.@Deployment of the system must be possible in various configurations but all of them need to fulfil basic requirements	• SubSys Plan Execution shall have generic application logic that works independently of the content of the Map Data, if the structure of the Map Data is respected • SubSys Plan Execution shall 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 violating the RAMSS specifications • SubSys Plan Execution shall have a strong separation of SW and HW concerns	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	• SubSys Plan Execution shall provide generic capability-based interfaces	Concept: TBD
A.P.M.@Standardize all main CCS processes, functionalities and interfaces	• SubSys Plan Execution shall use standardised interfaces for communication with other (sub-)systems	Concept: TBD
A.P.M.@Support a broad applicability to different railways and in various types of traffic and operational processes	• SCI-OP shall be independent from operational processes • SCI-OP shall support different kinds and granularities of Operational Plans independent from provided functionality and behaviour of the Physical Train Units and Field Elements	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]

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	• SubSys Plan Execution shall provide generic capability-based interfaces	Concept: TBD
A.P.M.@Use secure standard protocols	• SubSys Plan Execution shall use standardised interfaces for communication with other (sub-)systems	Concept: TBD
A.P.M.@Use standardized processes and systems	• SubSys Plan Execution shall be developed according to EN 50128 and EN 50126-1 • SubSys Plan Execution shall be developed according to a Secure Development Lifecycle (SDL) process as defined in TS 50701 / IEC 62443-4-1 • SubSys Plan Execution shall use standardised interfaces for communication with other (sub-)systems	Concept: TBD
A.P:M.@Implement ATO GoA2 or GoA3-4	• SCI-OP shall support different ATO levels (GoA1 – GoA4) and ETCS levels (L2/L3) and a mixed level approach	Concept: Standard Communication Interface Operational Plan [RCA.Doc.31]
A.P.M.@Reduce the number of individual systems, components, field elements sharing non-standardised interfaces	• SubSys Plan Execution shall work independently of the functionality of neighbouring SubSys, therefore no assumptions about dedicated behaviour shall be made	Concept: TBD Concept: Architectural Design for Plan Execution [RCA.Doc.49] Functional concept: TBD
	• SubSys Plan Execution shall use standardised interfaces for communication with other (sub-)systems	Concept: TBD

3.9. Category: Usability

Table 15: Usability Objectives and Systems Requirements A.P.M.

Objectives A.P.M	System Requirements	Reference to Concept
A.P.M.@Provide state of the art usability for GUI operations (incl. comfort functions such SSO)	• SubSys Plan Execution shall support a cross-system Single-Sign-On (SSO). • SubSys Plan Execution GUI shall be developed according to User Experience (UX) methods Note: It is not yet decided whether SubSys Plan Execution GUI will be implemented by SubSys Plan Execution or SubSys Workbench. Therefore, it is possible that the requirements regarding the GUI will transferred to the SubSys Workbench.	Concept: TBD
A.P.M.@Allow integration of GUI for all APM systems, which allows a cross-system overview and quick change between operated systems	• SWI-PE shall support the integration into a superordinated GUI.	Concept: TBD
A.P.M.@Ensure synchronized state between GUI of all APM systems	• SubSys Plan Execution shall be able to provide its System State and Operational State to other RCA SubSys	Concept: Architectural Design for Plan Execution [RCA.Doc.49]

4. PRAMSS

4.1. Performance and RAMSS Requirements

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

4.1.1. Performance

This section will be further elaborated in future releases.

4.1.2. 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 will also be affected.

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.

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 to enable reliability analysis.

4.1.3. Availability

System availability depends on hardware and software availability. This chapter is dealing with software availability only. Software availability can be measured during system operation. The quantitative prediction of software availability cannot be done seriously at this stage.

In principle, 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 to enable availability analysis.

4.1.4. 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 fault 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.

4.1.5. 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.

4.1.6. Security

SubSys PE shall be developed according to TS 50701 which describes how the IEC 62443 standard shall be applied for Railway Systems.

4.1.6.1. Secure Development Lifecycle

TS 50701 defines that the components (in terms of RCA subsystems) of the Railway Systems shall be developed according to IEC 62443. Therefore, for the development of the SubSys PE, a Secure Development Lifecycle (SDL) according to IEC 62443-4-1 shall be applied.

4.1.6.2. Security Requirements

TS 50701 defines that on (Railway) system level risk assessments shall be done and based on this, security zones and conduits shall be defined. For every zone and conduit, the Security Level (SL) and dedicated security requirements are then defined based on the risk assessments. Therefore, SubSys PE shall:

- Implement the security requirements derived from the risk assessment (not yet defined)
- Implement the functional requirements defined in IEC 62443-4-2 according to the Security Level of the zone SubSys PE is located in.

4.2. RAMSS Policies and Targets

General note: RAMSS policies and targets will be examined in an overall RCA analysis.

4.3. Safety Legislation

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

Table 16: Safety Legislation

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') In particular, consideration of Article 6 - Common safety methods ('CSMs').

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

4.4. Impacts from further Regulations

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

4.5. Assumptions and Justifications

None.

5. Issues

Table 17: Issues

Nr.	Title	Description
1	-	-