RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

System Concept ATO Execution

Document id: RCA.Doc.73

Table of contents

List of Figures

List of Tables

Version history

Version	Date	Author	Description
<2.0>	<16/08/2022>	Albrecht Achilles, Martin Kemkemer, and other members of the RCA-OPE-Cluster and the RCA-ATO-Cluster	Initial set up including review and revision cycles
<3.0>	<01.09.2022>	Albrecht Achilles, Martin Kemkemer, and other members of the RCA-OPE-Cluster and the RCA-ATO-Cluster	Ready for release

1. Introduction

1.1. Release information

Basic document information:

RCA-Document Number: RCA.Doc.73
Document Name: System Concept ATO Execution
Cenelec Phase: 1
Version: 3.00
RCA Baseline set: BL0
Approval date: 01.09.2022

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

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 Automatic Train Operation (ATO) Execution (in the following SubSys AE), as one part of the trackside ATO systems beside the SubSys ATO Transactor (in the following SubSys AT).

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

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

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 explicitly with red italic notes as this:

This section will be further elaborated in future releases.

2. System

The definition of the system under consideration, SubSys AE is performed in the following steps:

1. Definition of high-level scope, especially by definition of what is out of scope
2. Definition of the context
3. Definition of environment and boundaries, including the interfaces, surrounding systems, human actors, and economic respectively legal aspects
4. Definition of high-level system functionality derived from business goals and subsystem Use cases

2.1. Scope

2.1.1. In Scope

The core functionality of SubSys AE is the automatic and precise transaction and execution of the Operational Plan data sent by the external Planning System (PAS).

- SubSys AE timely transacts operational movements defined in the Operational Plan towards the further ATO infrastructure and ATO-OB for execution.
- SubSys AE transacts ATO-OB status reports received from SubSys AT back to PAS via train unit reports

The final scope of SubSys AE functionality is still under consideration.

As a connecting SubSys between PAS and SubSys AT the SubSys AE makes a decisive contribution to RCA so that the overall system can benefit from new technical possibilities of ATO railway operation.

The coordination with the processing of the SubSys Plan Execution (PE) and the following downstream systems is assured, by using the same Operational Plan instance sent by PAS and the synchronisation of the execution on onboard. SubSys AE is based on the exported constraint that SubSys PE and the following downstream systems fulfil the requirement to secure any train movement at any time.

2.1.2. Out of scope

Following the RCA architecture, the ATO trackside system, including SubSys ATO Execution and SubSys AT is not part of the safety related railway operation system chain.

Furthermore, following the definition of the RCA architecture the Planning System (PAS) and the functions listed in this chapter are not part of the scope of SubSys AE, although these functions might be included in current systems or system specification such as ATO-Trackside (ATO-TS) following Subset-125 [1]. The list is not exhaustive and may still change due to the adapted architecture.

Operational Plan management

- SubSys AE 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, only.
- SubSys AE does not support Operational Plan that offer different variants for the given Track Path from the departure to the arrival position. SubSys AE only supports track-exact Operational Plans.
- SubSys AE does not check the Operational Plan against compatibility nor vehicle data nor other analogue data. But SubSys AE does perform a validity check of Operational Plan data against the valid Map Data stored in SubSys AE.

Communication and management of ATO-onboard

- SubSys AE does not provide ATO infrastructure data (especially Subset-126 format [2]) to other RCA subsystems. SubSys AE only uses the provided Map Data, including the ATO specific data, from DCM for internal functions, like validity check of the specific Operational Plan data, conversion of Operational Plan data or conversion of ATO-OB reports into SCI-OP (see chapter 2.4.3.2)

Communication and management of ATO-onboard

- SubSys AE does not manage the communication sessions between ATO-OB and SubSys AT
- SubSys AE does not manage single vehicles or ATO-OB units

2.2. Context

2.2.1. RCA

1. SubSys AE is specified in the RCA. In terms of the overall RCA, it is a sub system (SubSys).
2. SubSys AE is envisaged as a non-safety-relevant system.
3. The development process should be done according to EN 50126-1 [8] and EN 50128 [10] 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.
4. As part of RCA the SubSys AE is intended for international use by European railway Infrastructure Managers.
5. SubSys AE is specified synchronously with other SubSys in the RCA and is connected to adjacent SubSys via defined interfaces.
6. With the SCI-OP, SubSys AE provides the interface that defines one system boundary from RCA to the Planning System (PAS).
7. For the development of SubSys AE and the related interfaces the compliance with international standards (e.g. Subset-125 [1], TSI TAF/TAP [11]) is to be observed.
8. SubSys AE is designed as highly available system. The actual availability requirements will be determined on basis of the required RAM analysis.
9. SubSys AE is operated together with exactly one logical instance of a Planning System and one or many logical instances of SubSys AT. (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 managed by a single RCA system, thus achieving scalability). In case a SubSys AE instance controls more than one SubSys AT instance, SubSys AE must split JPs, to provide each SubSys AT instance with an JP fitting to its area of control.

2.2.2. Operation and training

The main scope of SubSys AE is the ATO related technical communication between the Planning System and the further ATO downstream systems, especially SubSys AT.

There will be no railway operation performed manually at the SubSys AE. Therefore, there will be no operational regulation nor training required for railway operator in relation to the SubSys AE.

Furthermore, the SubSys AE maintenance and configuration processes will be executed remotely via the RCA support SubSys DCM, DM and IAM. Therefore, there will be no operational regulation nor training required for maintenance and configuration operator in direct relation to the SubSys AE.

But the regulation and training for maintenance and configuration of SubSys AE must be provided to the responsible personnel of the RCA support SubSys DCM, DM and IAM. This is not in scope of this document and must be evaluated in later development phases.

2.2.3. Organisation

SubSys AE 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 AE 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 & Boundary

2.3.1. Physical influences

SubSys AE consists of hardware or virtual environment and software. The hardware component, if used, might be exposed to physical influences.
There is no railway operation performed manually at the SubSys AE, therefore there is also no physical input-output devise specified in this relation.
Maintenance and configuration tasks might be performed via physical input-output devise part of the SubSys AE, which might be exposed to physical influences. But it is assumed, that all maintenance and configuration tasks will be performed remotely (see chapter 2.4.3.8 SubSysUC8 Remote operation), not via a direct physical input-output devise of the SubSys AE.

2.3.2. Interfaced systems

According to the current RCA/OCORA Subsystem Architecture, see RCA.Doc.35, System Definition [21] and RCA.Doc.40, RCA Architecture Poster [23] (see Figure 1 and Figure 2) the SubSys AE is connected to several RCA SubSys and one system outside of the RCA system boundaries.

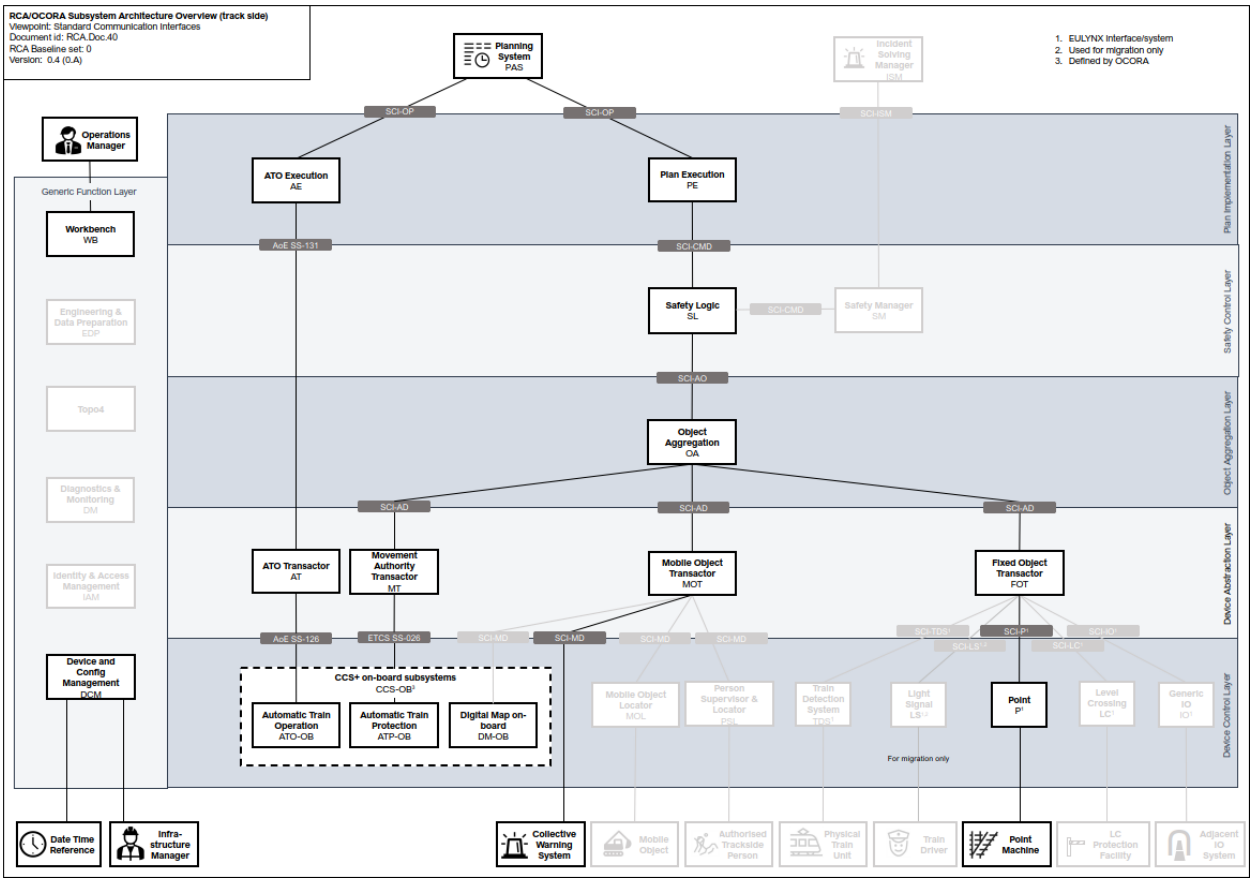

Figure 1: RCA/OCORA Subsystem Architecture Overview (Viewpoint: Standard Communication Interfaces)

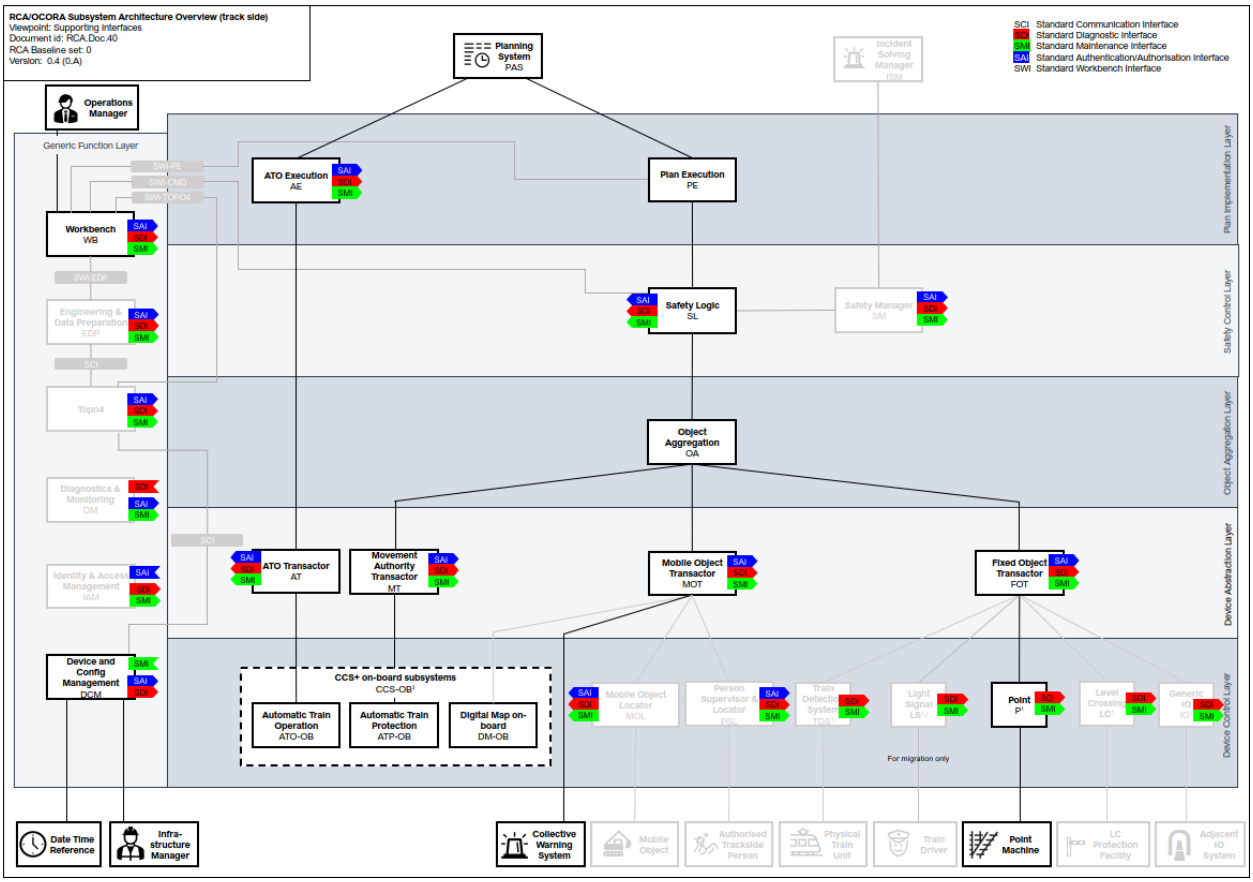

Figure 2: RCA/OCORA Subsystem Architecture Overview (Viewpoint: Supporting Interfaces)

In the following Table 1 the internal RCA SubSys and external system SubSys AE interacts with are listed. For all interfaced SubSys, detailed concepts and specifications either exist or are under development. Therefore, Table 1 only describes in brief the interfaces from and to SubSys AE.

Table 1: Interfaced SubSys of SubSys ATO Execution

ID	SubSys	Interfaces	Description
(1)	**PAS**	SCI-OP	The Planning System (PAS) is outside of the RCA system architecture and interfacing to the RCA system via the SCI-OP interface. PAS is the centralized system for railway operation and dispatching, including scheduling, conflict detection and solution. PAS operates the railway system, steering the railway operation via the Operational Plan (e.g. timetable) as input to the RCA system via the SCI-OP interface. The Operational Plan is distributed within RCA to the SubSys AE and the SubSys Plan Execution (PE). PAS receives status information from the RCA system (SubSys AE and the SubSys Plan Execution (PE)) regarding the processing and status of railway operation.

ID	SubSys	Interfaces	Description
(2)	**AT**	X2Rail-131 [4]	The SubSys AT is beside the SubSys AE the second subsystem of the ATO trackside (ATO-TS) following the general system architecture of the Subset-125 [1] within the RCA system architecture. SubSys AT manages the communication sessions with the ATO-OB. SubSys AT forwards status information from the ATO-OB, which have a ATO communication session to SubSys AT. SubSys AT receives operational plan data in the format of Journey Profiles from SubSys AE. In the RCA system architecture the interface is referenced as “AoE SS-131”. In the following the interface will be referenced as “X2Rail-131” according to the definition documentation [4]
(3)	**DCM**	SMI-AE	The SubSys Device & Configuration Management (DCM) is used to register, setup, and configure devices and RCA subsystems. This includes distributing and updating the configuration data and the software version to the RCA subsystems. Based on the SMI concept [22] configuration data are understood as railway configuration data (including inter alia Map Data, specific parameter data) and software configuration data (including inter alia communication parameters, security, and software data). SubSys DCM provides Map Data to the SubSys AE including all relevant infrastructure data. Map Data is provided to the consuming RCA subsystems. During the operation, the Map Data is used to support system specific functions, e.g. for support with On-Board localisation, generating ETCS movement authorities or other specific use cases. The Map Data includes a build-up set of edges along with associated nodes (e.g. points, buffer stops), the relevant infrastructure characteristics (e.g. curve radius and gradients), and location information (e.g. specific reference points, balises). The Map Data remain unchanged during operation phase until the next provisioning of Map Data. (For further definition see MAP Object Catalogue [24]. It is assumed, that SubSys DCM ensures coherent infrastructure data within all relevant RCA system systems. The scope of DCM will be further elaborated and defined in future releases.

ID	SubSys	Interfaces	Description
(4)	**DM**	SDI-AE	The SubSys Diagnostics & Monitoring (DM) collects monitoring and diagnostics information from the RCA subsystems Furthermore, for this concept document it is assumed that DM provides functionality for remote operation with the focus on maintenance. The scope of DM will be further elaborated and defined in future releases.
(5)	**IAM**	SAI-AE	The Identity and Access Management (IAM) authenticates and authorizes users and technical systems and grants or denies access to the Subsystems of the RCA system architecture. Therefore, IAM stores the credentials to authenticate the entities. The scope of IAM will be further elaborated and defined in future releases.

2.3.3. System interfaces

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

2.3.3.1. 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 Plan Execution and SubSys AE. The Planning System sends Operational Plans via the SCI-OP to be implemented by SubSys Plan Execution and SubSys AE. SubSys Plan Execution and SubSys AE will provide information about the execution progress of the Operational Plans and the actual state of railway operations in the Area of Control.
- **Downstream:**
  - Operational Plan Execution Request 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 (entity: Train Unit Report)

2.3.3.2. X2Rail-131

The naming of “X2Rail-131” is to be understood as a placeholder for the documentation of the interface between the RCA SubSys AE and SubSys AT. It must be decided, which documentation finally to be used, the X2Rail-131 [4], related documents or new documents.

- **Full name:** ATO-TS / TMS Interface Specification
- **Description:**

- The interface X2Rail-131 is part of the Reference CCS Architecture between the RCA Sub-Sys AE and SubSys AT. In the understanding of this interface X2Rail-131 the ATO-TS of Subset-125 [1] is to be mapped to SubSys AT of RCA.
- The interface X2Rail-131 is still under development.

- **Downstream:**
  - Journey Profile
- **Upstream:**
  - Receive Status Report Data, Connection Report, Journey Profile Request

2.3.3.3. SMI

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA.Doc.35, System Definition [21] and Concept SMI, RCA.Doc.74 [22], for details.

2.3.3.4. SDI

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA.Doc.35, System Definition [21], for details.

2.3.3.5. SAI

- Description is in responsibility of Architecture-Cluster.
  Please refer to RCA.Doc.35, System Definition [21], for details.

2.3.4. System multiplicity

For the definition of the system multiplicity the following assumptions are made:

1. Multiplicity PAS to SubSys AE = 1:m
   a. One PAS instance is capable to control several RCA instances and, in this relation, several SubSys AE instances
2. Multiplicity SubSys AE to SubSys AT = 1:n
   a. One SubSys AE instance is capable to control several SubSys AT instances
3. Multiplicity SubSys AT to ATO-OB = 1:p
   a. One SubSys AT instance is capable to control several SubSys ATO-OB instances

This might result in a system setting as shown exemplary in Figure 3.

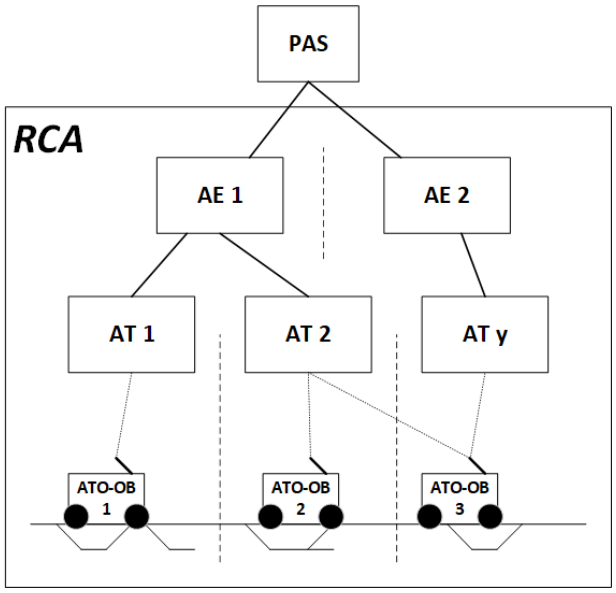

Figure 3: System multiplicity

2.3.5. Human actors

There is no railway operation performed manually at the SubSys AE, therefore there is also no human actor in this relation.
Maintenance and configuration tasks might be performed manually, either via physical input-output devise as part of the SubSys AE or remotely. Therefore, human actors with the role of maintainer and system administration might be necessary. For the further description only the SubSys DM, SubSys DCM and SubSys IAM are defined as actors and it is assumed, that any interaction of human actors is performed via these SubSys.

2.3.6. 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 AE 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 AE 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.

2.4. Business goals, Use cases & Functions

In the following chapters the Use cases and functions of the SubSys AE are derived from the RCA business goals, measures and basic architectural definitions.

2.4.1. RCA Business Goals and measures

As part of the ATO overall system, SubSys AE supports the overall RCA Business Goals and Objectives (see chapter 2, RCA.Doc.48 Realization of RCA Goals [6]).

SubSys AE as part of the ATO overall system contributes with a set of measures to reach the RCA goals. These measures are inter alia the following functional capabilities (see chapter 3, RCA.Doc.48 [6]):

1. F3: Automatic driving from start location to stop location GoA2
2. F12: Provide detailed information about degraded situation to TMS (e.g. such that TMS can estimate the duration)
3. F13: Provide continuous speed and position of all train units to interested actors

Furthermore, SubSys AE contributes to the Quality Attributes and the Architectural Principles as defined in chapters 3.3.1. and 3.3.2. in RCA.Doc.48 [6].

The above-mentioned measures are broken further down and detailed on system architecture level as defined in the RCA.Doc.35, System Definition [21], chapter 3.7.7. SubSys AE of the RCA System Architecture. The basic architectural definitions for the SubSys AE are:

1. Translates Operational Plan to Journey Profile
2. Supports different automation level
3. Operates on abstract representations of real-world elements
4. Operates in real-time

2.4.2. Subsystem Use cases

Based on the RCA business goals, measures and basic architectural definitions as summarized above in chapter 2.4.1 subsystem Use cases are defined for the SubSys ATO Execution as shown in Figure 4 and listed below in Table 2.

Subsystem Use cases are not a part of the final modelling but are used to structure this document.

Table 2: Subsystem Use cases of SubSys ATO Execution

ID	Subsystem Use cases	Brief Description
SubSysUC1	*Maintain Journey Profiles*	Subsystem Use case to receive and to transform PAS Operational Plan data into the ATO specific format of Journey Profile (JP), to provide JP to the SubSys AT including the management of JP transmission status and local storage of JPs.
SubSysUC2	*Maintain AE Map Data*	Subsystem Use case to load, update and activate Map Data from SubSys DCM.
SubSysUC3	*Handle Connection Status Report*	Subsystem Use case to receive and to transform status changes of ATO communication sessions (connection) between an ATO-OB and a SubSys AT instance and to provide this information as Train Unit Report to PAS.
SubSysUC4	*Handle Status Reports*	Subsystem Use case to receive and to transform ATO Status Report information (according to Subset-126 [2]) of an ATO-OB via SubSys AT instance and to provide this information as Train Unit Report to PAS.
SubSysUC5	*Handle Train Capability Report*	The SubSysUC5 Handle *Train Capability Report* is moved to the open points list, see chapter 4, ID5.

ID	Subsystem Use cases	Brief Description
		Subsystem Use case to receive and to transform Train Capability Report information of an ATO-OB via SubSys AT and to provide this information as Train Unit Report to PAS. This Use case is optional.
SubSysUC6	*AT/AE responsibility management*	Intentionally deleted
SubSysUC7	*Maintain Diagnostic Data and Error*	Subsystem support Use case to acquire detailed information of the SubSys AE system status including all involved hardware and software components and interfaces. This includes the logging of all interface status and communication data available. SubSys AE provides diagnosis and status data to external clients.
SubSysUC8	*Remote operation*	Subsystem support Use case to maintain an SubSys AE instance via a remote interface. This includes at minimum start / stop / restart functions of the SubSys AE application and computation unit (hardware or virtual environment). Furthermore, update and configuration of the SubSys AE software application are part of the basis functionality covered by this subsystem Use cases.
SubSysUC9	*Identity & Access Management*	Subsystem support Use case to maintain and to control access rights to the service function of the SubSys AE. Various standard roles are used to determine which user group has access the functions/data of the logging and remote operation interface.

The actors shown in Figure 4 represent the systems interfaced to and interacting with SubSys AE, as described in chapter 2.3.2 above.

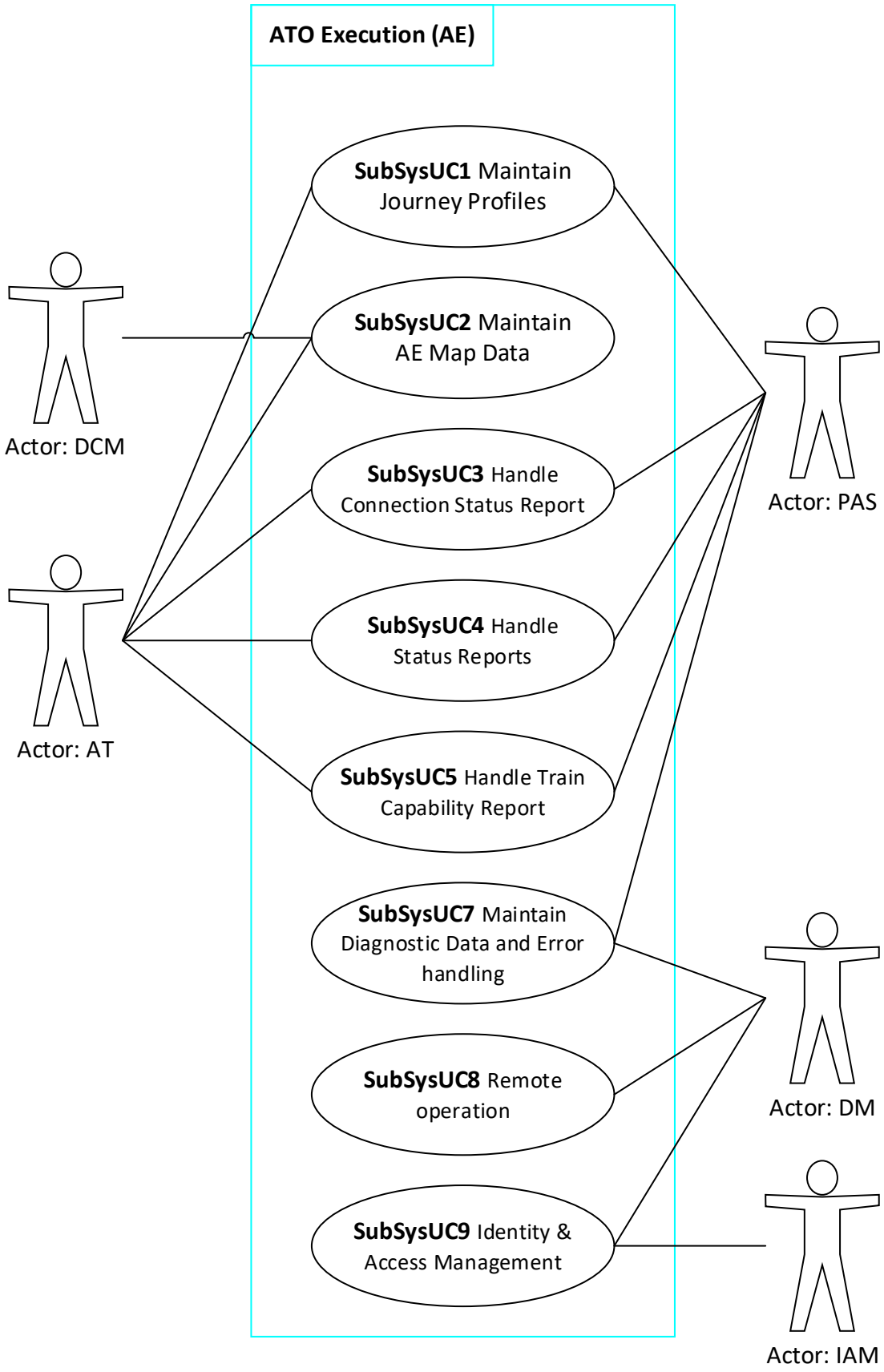

Figure 4: SubSys AE Subsystem Use cases[1]

2.4.3. High-level Functional Process flows

Along the above-described subsystem Use cases (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**) the high-level functional process flows are sketched and descripted in the following subchapters.

For each subsystem Use case the following perspectives are described:

1. (Main) goal to be achieved by the subsystem Use case
2. Assumptions, that are made for the subsystem Use case, if any
3. Exported constraints and requirements, any kind of requirements that are raised to interfaced systems or the interface as such. The exported constraints and requirements must be processed and detailed further by the system concerned.

Please note, that the presented process flows focus on the interfaces and basic workflows but are not comprehensive representations of internal data flows.

The SubSys AE system functions, which are mentioned in the following functional process flows are listed and described further in chapter 2.4.4 High-level processual system .

[1] **Disclaimer**: The presented modelling is only modelled for illustration of concepts and is not yet aligned with MBSE Methodology.

2.4.3.1. SubSysUC1 Maintain Journey Profiles

2.4.3.1.1. Subsystem Use case Goal

The goal of SubSysUC1 *Maintain Journey Profiles* is to provide functions to receive and to transform PAS Operational Plan data into the ATO specific format of Journey Profile (JP), to provide JP to the SubSys AT including the management of JP transmission status and local storage of JPs.

2.4.3.1.2. Functional process flow

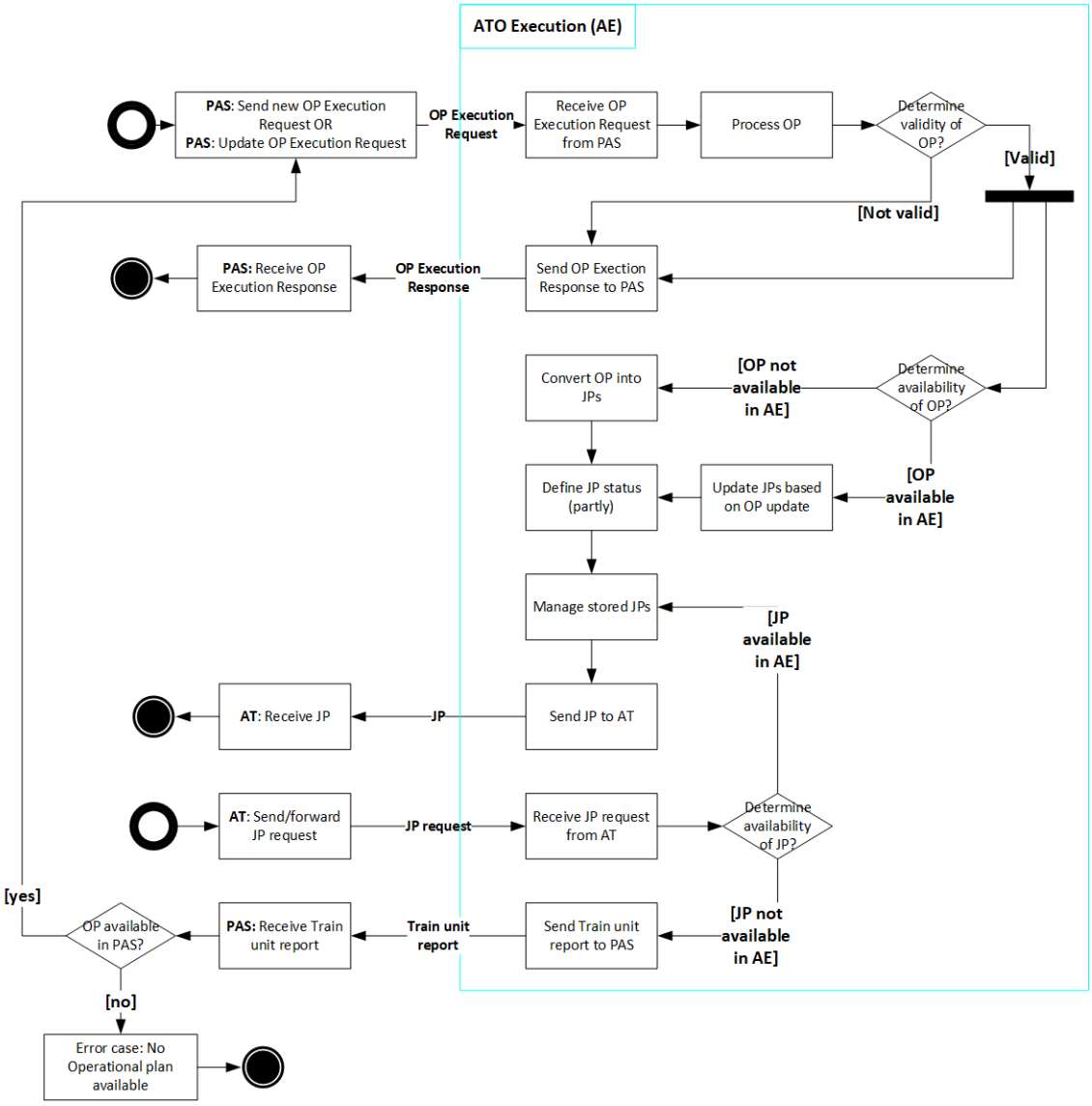

Figure 5: Process flow of SubSysUC1 Maintain Journey Profiles

2.4.3.1.3. Exported constraints / requirements

In relation to the functional process flow of SubSysUC1 *Maintain Journey Profiles* exported constraints and requirements as listed in Table 3 must be considered:

Table 3: SubSysUC1 – exported constraints / requirements

ID	System	Description
SubSysUC1-EXCR-1	ATO-OB/AT	SubSys ATO-OB and SubSys AT shall process JP request and JP according to Subset-126 [2] SubSys AT shall manage JPs send by SubSys AE in case necessary before sending it to SubSys ATO-OB.

ID	System	Description
SubSysUC1-EXCR-2	SCI-OP	Interface SCI-OP shall provide any Operational Plan data necessary to compile JP according to Subset-126 [2]
SubSysUC1-EXCR-3	SCI-OP	Interface SCI-OP shall implement a new message Train Unit Report with the special meaning of a JP request or request for Operational Plan data to PAS
SubSysUC1-EXCR-4	X2Rail-131	Interface X2Rail-131 shall transmit JP, JP request message according to Subset-126 [2]
SubSysUC1-EXCR-5	PAS	External system PAS or processes on the PAS level shall manage the error case, that no Operational Plan data is available for an existing train (e.g. train running number unknown or wrong train number entered). Although the error is originated on the onboard level, it is assumed that the solution is only possible on PAS level. The error case must be differentiated whether it occurs during start up or during an update of JP during an ongoing ATO run.
SubSysUC1-EXCR-24	DCM	SubSys DCM shall ensure that the Map Data relevant for the SubSys AE instance are available and up to date in SubSys AE. It is mandatory that SubSys AE and the SubSys AT operate on the same Map Data version at any given time.

2.4.3.2. SubSysUC2 Maintain AE Map Data

Due to the ongoing definition of functionalities and the processes around the SubSys Device & Configuration Management system (DCM) the SubSys AE subsystem Use case SubSysUC2 *Maintain AE Map Data* is not detailed in a process flow.

For further details it must be referred to the following documents:

1. RCA.Doc.54, Solution Concept: MAP [20]
2. RCA Modell, System Capability 87 [21]
3. RCA.Doc.74, Concept SMI (not released yet) [22]

Based on the existing definition of functionalities and the processes of the SubSys Device & Configuration Management system the SubSys AE will implement as least the following system functions:

1. Pre-load of Map Data
2. Activation of Map Data

For further definition of these functions please refer to the definitions made for the SubSys DCM, as defined inter alia in the documents mentioned above.

SubSys DCM provides Map Data to the SubSys AE including all relevant infrastructure data in the generic Map Data format.

SubSys AE uses the Map Data inter alia as basis for the following functions:

1. Validity check of the specific Operational Plan in relation to the current Map Data version (see chapter 2.4.3.1)
2. Conversion of Operational Plan into the Subset-126 [2] format (Journey Profiles (JP)) (see chapter 2.4.3.1)
3. Conversion of Reports from ATO-OB into SCI-OP related data format (see chapter 2.4.3.3, 2.4.3.4, 2.4.3.5

2.4.3.3. SubSysUC3 Handle Connection Status Report

2.4.3.3.1. Subsystem Use case Goal

The goal of SubSysUC3 to provide functions to receive and to transform status changes of ATO communication sessions (connection) between an ATO-OB and a SubSys AT instance and to provide this information as Train Unit Report to PAS.

2.4.3.3.2. Functional process flow

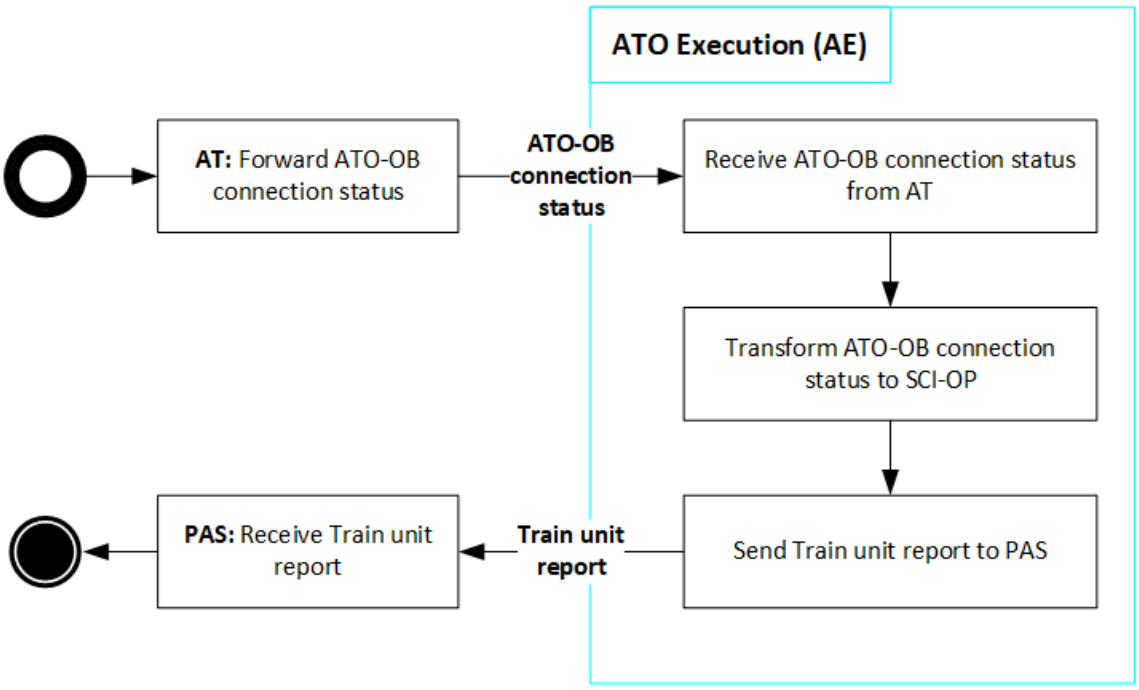

Figure 6: Process flow of SubSysUC3 Handle Connection Status Report

2.4.3.3.3. Exported constraints / requirements

In relation to the functional process flow of SubSysUC3 *Handle Connection Status Report* exported constraints and requirements as listed in Table 4 must be considered:

Table 4: SubSysUC3 – exported constraints / requirements

ID	System	Description
SubSysUC3-EXCR-6	ATO-OB/AT	SubSys ATO-OB and SubSys AT shall process the connection status of the related ATO communication session
SubSysUC3-EXCR-7	SCI-OP	Interface SCI-OP shall implement the message Train Unit Report to transmit connection status information of the related ATO communication session

2.4.3.4. SubSysUC4 Handle Status Reports

2.4.3.4.1. Subsystem Use case Goal

The goal of SubSysUC4 is to provided functions to receive and to transform ATO Status Report information (according to Subset-126 [2]) of an ATO-OB via SubSys AT instance and to provide this information as Train Unit Report to PAS.

2.4.3.4.2. Functional process flow

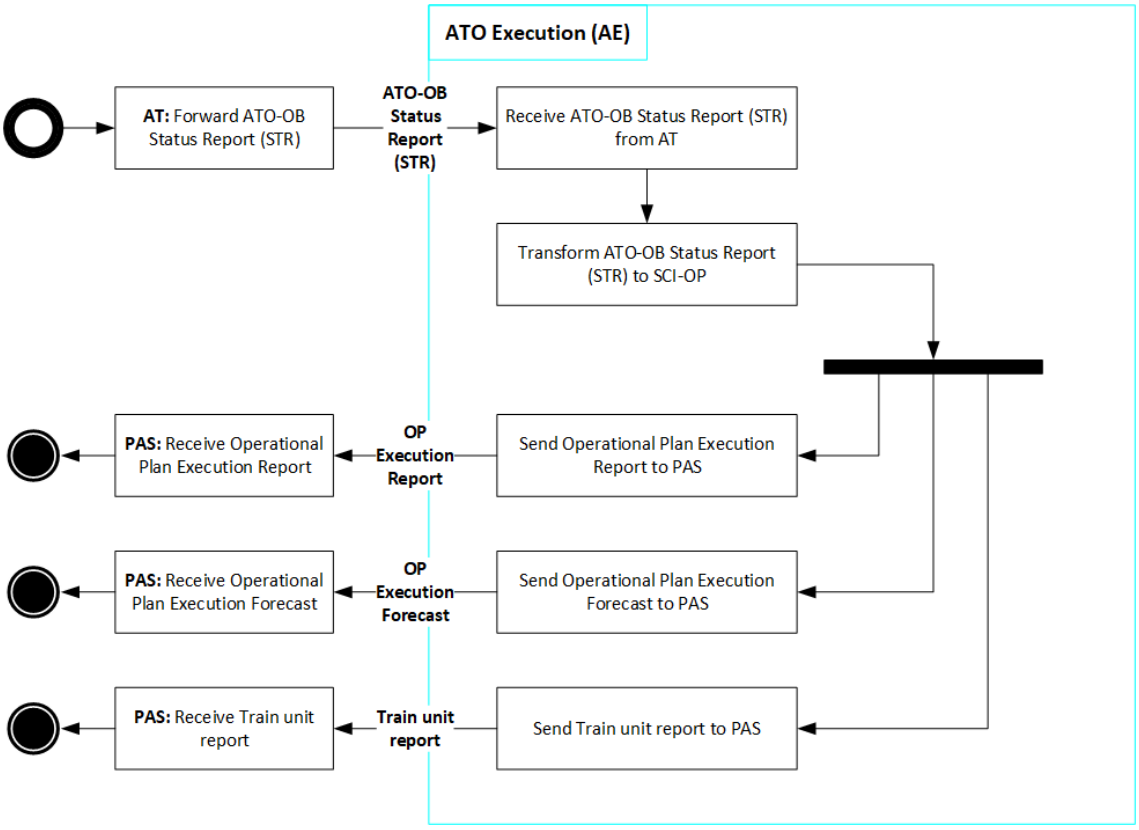

Figure 7: Process flow of SubSysUC4 Handle Status Reports

2.4.3.4.3. Exported constraints / requirements

In relation to the functional process flow of SubSysUC4 *Handle Status Reports* exported constraints and requirements as listed in Table 5 must be considered:

Table 5: SubSysUC4 – exported constraints / requirements

ID	System	Description
SubSysUC4-EXCR-8	ATO-OB/AT	SubSys ATO-OB and SubSys AT shall process the ATO Status Report of the ATO-OB
SubSysUC4-EXCR-9	SCI-OP	Interface SCI-OP shall implement messages to transmit ATO Status Report information of the related ATO-OB

2.4.3.5. SubSysUC5 Handle Train Capability Report

The SubSysUC5 Handle *Train Capability Report* is moved to the open points list, see chapter 4, ID5.

2.4.3.6. SubSysUC6 AT/AE responsibility management

Intentionally deleted

2.4.3.7. SubSysUC7 Maintain Diagnostic Data and Error

2.4.3.7.1. Subsystem Use case Goal

The goal of SubSysUC7 *Maintain Diagnostic Data and Error* is to acquire detailed information of the SubSys AE system status including all involved hardware and software components and interfaces. This includes the logging of all interface status and communication data available. SubSys AE provides diagnosis and status data to external clients.

2.4.3.7.2. Functional process flow

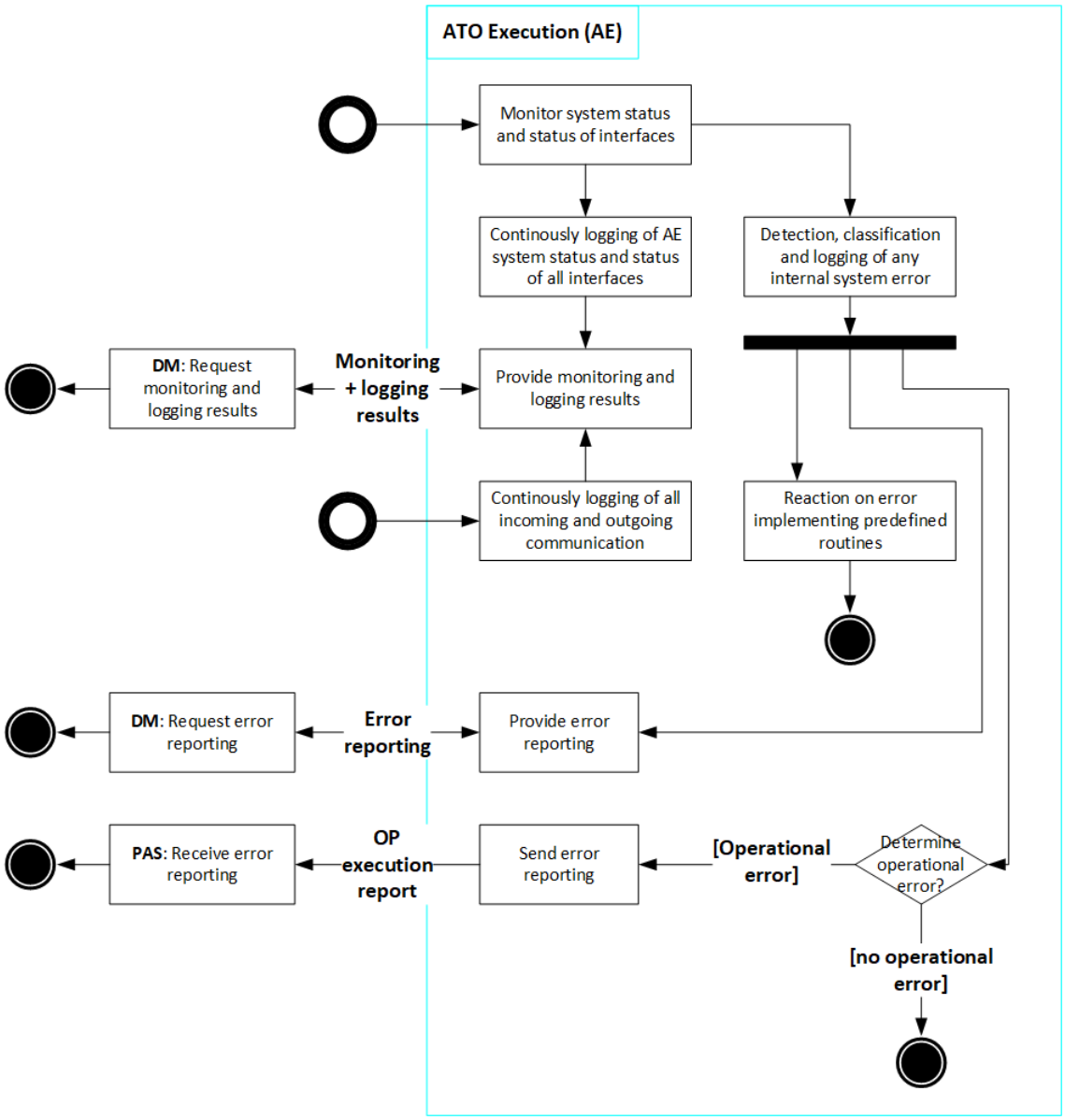

Figure 8: Process flow of SubSysUC7 Maintain Diagnostic Data and Error

2.4.3.7.3. Assumptions

For the definition of the functional process flow of SubSysUC7 *Maintain Diagnostic Data and Error* the assumption is made, that a server / slave mechanism (e.g. OPC Unified Architecture (OPC UA) structure) is implemented in the SubSys AE.

The access right to the diagnostic and error data is managed via the SubSys IAM, see SubSysUC9 *Identity & Access Management* in chapter 2.4.3.9.

2.4.3.7.4. Exported constraints / requirements

In relation to the functional process flow of SubSysUC7 *Maintain Diagnostic Data and Error* exported constraints and requirements as listed in Table 6 must be considered:

Table 6: SubSysUC7 – exported constraints / requirements

ID	System	Description
SubSysUC7-EXCR-14	DM	SubSys DM shall request monitoring and logging results, which are provided by SubSys AE
SubSysUC7-EXCR-15	DM	SubSys DM shall request error reporting, which is provided by SubSys AE

ID	System	Description
SubSysUC7-EXCR-16	DM	SubSys DM shall implement a server / slave mechanism to request monitoring, logging, and error data, which are provided by SubSys AE. SubSys AE is acting as server, providing these data to any (client) system, which subscribe to the SubSys AE server.
SubSysUC7-EXCR-17	SCI-OP	Interface SCI-OP shall implement the error reporting to PAS using a specific OP execution report message including error state.

2.4.3.8. SubSysUC8 Remote operation

Within the frame of the RCA development the functionalities of remote operation, allocated to SubSys Diagnostics & Monitoring (DM) are not yet defined in detail. Therefore, the SubSysUC8 *Remote operation* of the SubSys AE system is not detailed in a functional process flow.

The goal of the SubSysUC8 *Remote operation* is to enable remote operation for maintenance etc. for the SubSys AE. The minimum set of functions in this relation is:

1. Start / stop / restart functions of the SubSys AE application and computation unit (hardware or virtual environment)
2. Update and configuration of the SubSys AE software application

The access right to the remote operation is managed via the SubSys IAM, see SubSysUC9 *Identity & Access Management* in chapter 2.4.3.9.

2.4.3.9. SubSysUC9 Identity & Access Management

Within the frame of the RCA development the functionalities of Identity & Access Management allocated to SubSys IAM are not yet defined in detail. Therefore, the SubSysUC9 *Identity & Access Management* of the SubSys AE system is not detailed in a functional process flow.

The goal SubSysUC9 *Identity & Access Management* is to enable identity management as part of security processes for the SubSys AE. The minimum set of functions in this relation is:

1. Authentication and authorisation of users and technical systems and granting / denying access to the SubSys AE.
2. Therefore, IAM stores the credentials to authenticate the entities.
3. The scope of IAM will be further elaborated and defined in future re-leases.

Table 7: SubSysUC9 – exported constraints / requirements

ID	System	Description
SubSysUC7-EXCR-25	IAM	IAM shall manage the access right for the access to the diagnostic and error data within SubSys AE
SubSysUC8-EXCR-26	IAM	IAM shall manage the access right for the remote operation functions within SubSys AE

2.4.4. High-level processual system functions

In the following Table 8 the processual system functions of SubSys AE, identified within the functional process flows per subsystem Use case are described on a high-level. The description is only meant to provide an indication and no detail design. The detailing must be performed in the subsequent development phases.

Table 8: High-level description of system function

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC1-AE-3	SubSysUC1	Receive OP Execution Request from PAS	SubSys AE receives Operational Plan (OP) data from PAS, either as new OP or as update of an already existing OP. The OP data received by SubSys AE are the same data as provided to the SubSys PE, to ensure synchronous information.	SCI-OP	Operation Plan Execution Request
ATO-SubSysUC1-AE-4	SubSysUC1	Process OP	SubSys AE processes the received OP at least by: 1. Performing the validity check of the OP data 2. Compiling the OP Execution Response message		
ATO-SubSysUC1-AE-80	SubSysUC1	Determine validity of OP?	SubSys AE checks, whether the specific Operational Plan is valid in relation to the current Map Data version. But SubSys AE does not check the Operational Plan against compatibility nor vehicle data nor other analogue data.		
ATO-SubSysUC1-AE-5	SubSysUC1	Send OP Execution Response to PAS	SubSys AE sends the OP Execution Response message to PAS as reaction to the received OP	SCI-OP	Operation Plan Execution Response
ATO-SubSysUC1-AE-7	SubSysUC1	Determine availability of OP?	SubSys AE checks, whether the specific Operational Plan is available in SubSys AE.		

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC1-AE-8	SubSysUC1	Convert OP into JPs	In case the specific Operational Plan is not available, SubSys AE converts the OP data into to the ATO data format of JPs (according to X2Rail-131 [4], respectively Subset-126 [2]). The final conversion to the Subset-126 [2] format fit for transmission to ATO-OB is performed by SubSys AT. In case the OP covers more than one specific SubSys AT instance, the specific SubSys AE is responsible for, the SubSys AE splits the OP into dedicated JP parts. As a result of the split, SubSys AE provides to each SubSys AT instance the dedicated JP related to the SubSys AT fitting to its area of control. The conversion is based on the current version of the Map Data.		
ATO-SubSysUC1-AE-9	SubSysUC1	Update JPs based on OP update	In case the specific Operational Plan is already available and was previously converted to JP format, SubSys AE updates the JP with the new OP data. In case an JP or a part of an JP was already sent to a responsible SubSys AT and with the update of the OP data, the SubSys AT is no longer responsible, SubSys AE must send a JP message to the SubSys AT, that indicates that the previously send JP is no longer valid and must be deleted.		
ATO-SubSysUC1-AE-10	SubSysUC1	Define JP status (partly)	SubSys AE defines the JP status. This JP status definition cannot be done finally, because some status definitions depend on the status of the ATO communication session between SubSys AT and ATO-OB and/or the shipping status of JP from SubSys AT to ATO-OB. This information is outside of the scope of SubSys AE, but within the scope of SubSys AT.		
ATO-SubSysUC1-AE-11	SubSysUC1	Manage stored JPs	SubSys AE stores and manages the JP locally within the specific SubSys AE instance.		
ATO-SubSysUC1-AE-12	SubSysUC1	Send JP to AT	SubSys AE sends the JP immediately, when it is processed in SubSys AE, to the SubSys AT.	X2Rail-131	JP
ATO-SubSysUC1-AE-15	SubSysUC1	Receive JP request from AT	SubSys AE receives JP request according to Subset-126 [2] from SubSys AT.	X2Rail-131	JP request
ATO-SubSysUC1-AE-16	SubSysUC1	Determine availability of JP?	SubSys AE checks, whether the specific JP is available in SubSys AE.		

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC1-AE-17	SubSysUC1	Send Train unit report to PAS	In case the specific JP is not available, SubSys AE sends a Train unit report via SCI-OP to PAS, which serves as a request for Operational Plan data for the specific JP request.	SCI-OP	Train unit report
ATO-SubSysUC2-AE-21	SubSysUC2	Pre-load of Map Data Versions	For further definition of the function please refer to the definitions made for the SubSys DCM, as defined inter alia in the documents listed in chapter 2.4.3.2.		
ATO-SubSysUC2-AE-22	SubSysUC2	Activate Map Data Version according to activation command	For further definition of the function please refer to the definitions made for the SubSys DCM, as defined inter alia in the documents listed in chapter 2.4.3.2.		
ATO-SubSysUC3-AE-24	SubSysUC3	Receive ATO-OB connection status from AT	SubSys AE receives the ATO-OB connection status report via SubSys AT related to the established ATO communication session.	X2Rail-131	ATO-OB connection status
ATO-SubSysUC3-AE-25	SubSysUC3	Transform ATO-OB connection status to SCI-OP	SubSys AE transforms the ATO-OB connection status report to the SCI-OP data format, by mapping it to the Map Data and converts it to SCI-OP, Train Unit Report format. SubSys AE divides and allocates the ATO-OB connection status report data to the different data formats of the SCI-OP interface, as Operational Plan Execution Report, Operational Plan Execution Forecast, Train unit report.	SCI-OP	
ATO-SubSysUC3-AE-26	SubSysUC3	Send Train unit report to PAS	SubSys AE sends the Train unit report to PAS	SCI-OP	Train unit report
ATO-SubSysUC4-AE-29	SubSysUC4	Receive ATO-OB Status Report (STR) from AT	SubSys AE receives the ATO-OB Status Report (STR) according to Subset-126 [2] via SubSys AT.	X2Rail-131	ATO-OB Status Report (STR)
ATO-SubSysUC4-AE-30	SubSysUC4	Transform ATO-OB Status Report (STR) to SCI-OP	SubSys AE transforms the ATO-OB Status Report (STR) to the SCI-OP data format, by mapping it to the Map Data and converts it to SCI-OP, Train Unit Report format. SubSys AE divides and allocates the ATO-OB Status Report (STR) data to the different data formats of the SCI-OP interface, as Operational Plan Execution Report, Operational Plan Execution Forecast, Train unit report.	SCI-OP	
ATO-SubSysUC4-AE-31	SubSysUC4	Send Operational Plan Execution Report to PAS	SubSys AE sends the Operational Plan Execution Report to PAS	SCI-OP	OP Execution Report

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC4-AE-33	SubSysUC4	Send Operational Plan Execution Forecast to PAS	SubSys AE sends the Operational Plan Execution Forecast to PAS	SCI-OP	OP Execution Forecast
ATO-SubSysUC4-AE-35	SubSysUC4	Send Train unit report to PAS	SubSys AE sends the Train unit report to PAS	SCI-OP	Train unit report
ATO-SubSysUC7-AE-60	SubSysUC7	Monitor system status and status of interfaces	SubSys AE monitors continuously the system status (SubSys AE application and computation unit (hardware or virtual environment)) and the status of all interfaces connected.		
ATO-SubSysUC7-AE-61	SubSysUC7	Continuously logging of AE system status and status of all interfaces	SubSys AE logs continuously the system status (SubSys AE application and computation unit (hardware or virtual environment)) and the status of all interfaces connected. The logging includes at least the valid time stamp and sufficient data to reconstruct the system status and status of all interfaces.		
ATO-SubSysUC7-AE-62	SubSysUC7	Continuously logging of all incoming and outgoing communication	SubSys AE logs continuously all incoming and outgoing interface communication The logging includes at least the valid time stamp and data exchanged during the communication.		
ATO-SubSysUC7-AE-63	SubSysUC7	Provide monitoring and logging results to DM	SubSys AE provides all monitoring and logging results via a server / slave mechanism (e.g. OPC Unified Architecture (OPC UA) structure) to any system, which subscribe to this service. SubSys AE acts as server for these information and functions.	SDI-AE	Monitoring + logging results
ATO-SubSysUC7-AE-65	SubSysUC7	Detection, classification, and logging of any internal system error	Based on the continuously monitoring of the system status (SubSys AE application and computation unit (hardware or virtual environment)) and the status of all interfaces SubSys AE detects any internal system error. When a system error is detected, SubSys AE classifies the system error according to a pre-defined classification mechanism and logs all related information. The logging includes at least the valid time stamp and sufficient data to reconstruct the error and the reactions performed by SubSys AE.		

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC7-AE-66	SubSysUC7	Reaction on error implementing predefined routines	SubSys AE activates pre-defined error reaction routines, corresponding to the detected system error. The pre-defined error reaction routines should try to limit the impact of the system error on railway operation.		
ATO-SubSysUC7-AE-67	SubSysUC7	Provide error reporting to DM	SubSys AE provides all information of the system error via a server / slave mechanism (e.g. OPC Unified Architecture (OPC UA) structure) to any system, which subscribe to this service. SubSys AE acts as server for these information and functions.	SDI-AE	Error reporting
ATO-SubSysUC7-AE-69	SubSysUC7	Determine operational error?	SubSys AE checks, whether the specific system error has an operational impact.		
ATO-SubSysUC7-AE-70	SubSysUC7	Send error reporting to PAS	In case the specific system error has an operational impact SubSys AE sends the relevant information of the system error to PAS, using a specific OP execution report message of the SCI-OP including the error state.	SCI-OP	OP execution report including error state
ATO-SubSysUC8-AE-72	SubSysUC8	Remote operation	Details of the overall SubSys AE function Remote operation are not defined yet. Please refer to chapter 2.4.3.8 for a first indication.		
ATO-SubSysUC9-AE-73	SubSysUC9	Identity & Access Management	Details of the overall SubSys AE function Identity & Access Management are not defined yet. Please refer to chapter 2.4.3.9 for a first indication.		

2.4.5. High-level Interface Description

In the following Table 9 the interface communications identified within the functional process flows per subsystem Use case are listed. The listing is only meant to provide an indication and no detail design. The detailing must be performed in the subsequent development phases.

Under the “Status” an indication for the current definition status of the interface communication is provided. The status is to be understood as the following:

1. “Defined”, the message / data defined in the functional process flows is already defined within the scope of the related interface communication.
2. “Extent”, the message / data used in the functional process flows must be extended by the data defined in the functional process flows within the scope of the related interface communication.
3. “Evaluate”, the interface communication as already defined must be evaluated in detail. It is assumed, that an extension of the interface communication is highly likely.

In any case detail definition and evaluation must be performed in the subsequent development phases.

Table 9: High-level description of SubSys AE interfaces

FCT-ID	SubSysUCID	Interface	Message	Start	Destina-tion	Status
ATO-SubSysUC1-PAS-1	SubSysUC1	SCI-OP	Operation Plan Execution Request	PAS	AE	Defined
ATO-SubSysUC1-PAS-2	SubSysUC1	SCI-OP	Operation Plan Execution Request	PAS	AE	Defined
ATO-SubSysUC1-AE-3	SubSysUC1	SCI-OP	Operation Plan Execution Request	PAS	AE	Defined
ATO-SubSysUC1-AE-5	SubSysUC1	SCI-OP	Operation Plan Execution Response	AE	PAS	Defined
ATO-SubSysUC1-AE-12	SubSysUC1	X2Rail-131	JP	AE	AT	Defined
ATO-SubSysUC1-AT-13	SubSysUC1	X2Rail-131	JP	AE	AT	Defined
ATO-SubSysUC1-AT-14	SubSysUC1	X2Rail-131	JP request	AT	AE	Defined
ATO-SubSysUC1-AE-15	SubSysUC1	X2Rail-131	JP request	AT	AE	Defined
ATO-SubSysUC1-AE-17	SubSysUC1	SCI-OP	Train unit report	AE	PAS	Extent
ATO-SubSysUC1-PAS-18	SubSysUC1	SCI-OP	Train unit report	AE	PAS	Extent
ATO-SubSysUC2-AE-21	SubSysUC2	SMI-AE	Map Data	DCM	AE	Extent
ATO-SubSysUC2-AE-22	SubSysUC2	SMI-AE	Activation command	DCM	AE	Extent
ATO-SubSysUC3-AT-23	SubSysUC3	X2Rail-131	ATO-OB connection status	AT	AE	Extent
ATO-SubSysUC3-AE-24	SubSysUC3	X2Rail-131	ATO-OB connection status	AT	AE	Extent
ATO-SubSysUC3-AE-26	SubSysUC3	SCI-OP	Train unit report	AE	PAS	Extent
ATO-SubSysUC3-PAS-27	SubSysUC3	SCI-OP	Train unit report	AE	PAS	Extent
ATO-SubSysUC4-AT-28	SubSysUC4	X2Rail-131	ATO-OB Status Report (STR)	AT	AE	Evaluate
ATO-SubSysUC4-AE-29	SubSysUC4	X2Rail-131	ATO-OB Status Report (STR)	AT	AE	Evaluate

FCT-ID	SubSysUCID	Interface	Message	Start	Destina-tion	Status
ATO-SubSysUC4-AE-31	SubSysUC4	SCI-OP	OP Execution Report	AE	PAS	Evaluate
ATO-SubSysUC4-PAS-32	SubSysUC4	SCI-OP	OP Execution Report	AE	PAS	Evaluate
ATO-SubSysUC4-AE-33	SubSysUC4	SCI-OP	OP Execution Forecast	AE	PAS	Evaluate
ATO-SubSysUC4-PAS-34	SubSysUC4	SCI-OP	OP Execution Forecast	AE	PAS	Evaluate
ATO-SubSysUC4-AE-35	SubSysUC4	SCI-OP	Train unit report	AE	PAS	Evaluate
ATO-SubSysUC4-PAS-36	SubSysUC4	SCI-OP	Train unit report	AE	PAS	Evaluate
ATO-SubSysUC7-AE-63	SubSysUC7	SDI-AE	Monitoring + logging results	AE	DM	Extent
ATO-SubSysUC7-DM-64	SubSysUC7	SDI-AE	Monitoring + logging results	AE	DM	Extent
ATO-SubSysUC7-AE-67	SubSysUC7	SDI-AE	Error reporting	AE	DM	Extent
ATO-SubSysUC7-DM-68	SubSysUC7	SDI-AE	Error reporting	AE	DM	Extent
ATO-SubSysUC7-AE-70	SubSysUC7	SCI-OP	OP execution report, including error state	AE	PAS	Extent
ATO-SubSysUC7-PAS-71	SubSysUC7	SCI-OP	OP execution report, including error state	AE	PAS	Extent

3. RAMSS

3.1. RAMSS Performance and Requirements

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

3.1.1. Reliability

SubSys AE 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 AE 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, supporting systems will observe the operation permanently and the reported reliability index (fault free calculations divided by all calculations) shall be 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 AE 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 AE needs to be able to process concurrent requests from interfaced systems. 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.
    - 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 AE, 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 supporting systems 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 principle, the availability depends on the reliability, a higher reliability leads to a higher availability. But even with the highest reliability there will be 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 AE 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 AE software itself. If SubSys AE 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.

For SubSys AE software, no quantitative prediction of availability will be made at this moment. Qualitative prediction can be made based on design principles. Furthermore, SubSys AE 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 AE 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 RCA.Doc.35, System Definition [21].
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 AE 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 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 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 AE 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. Safety

SubSys AE is envisaged as a non-safety-relevant system. It is not planned that SubSys AE assumes safety responsibility according to EN 50126-1 [8] or EN 50128 [10]. No safety targets are expected and thus no risk-minimising measures are envisaged.

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

- Validated risk analysis SubSys AE (EN 50126-1 [8] phase 3 for SubSys AE).
- Released overall system RCA risk analysis (EN 50126-1 [8] phase 3 for RCA).
- Released, final overall architecture RCA (EN 50126-1 [8] phase 5 for RCA).
- Released, final assignment of safety requirements / safety functions to RCA SubSys based on the architecture (EN 50126-1 [8] phase 5 for RCA).

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

3.1.5. 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 the ATO system. 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 AE is not foreseen.

This determination is preliminary.

Furthermore, the implementation of the overall security processes defined in the relevant standards EN 50126 [8]/[9], prTS 50701 [14], IEC 62443 [15] and VDEV 831-104 [16] as well as the EU-LYNX/RCA/OCORA guideline for cyber security [17] must be ensured.

3.1.6. 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 must be analysed and defined country specific.

3.3. Safety Legislation

3.3.1. Safety Regulations

The development of SubSys AE takes place according to the recognised rules of technology. Recognised rules of technology manifest themselves in standards. EN 50128 [10] 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 [10] applies to 'Railway applications – Telecommunications, signalling and data processing systems – Software for railway control and monitoring systems. SubSys AE is part of a railway operation system, non-application is generally not permitted.
Note: Further safety regulations must be analysed and defined country specific.

3.3.2. Identified legislation and their impact

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

Legislation	Impact on SubSys AE
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 [19]	Consideration of Interoperability
Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety [18]	Consideration of Common safety methods ('CSMs') In particular, consideration of Article 6 – Common safety methods ('CSMs').
EN 50128 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems [10]	Implement specifications and processes according to EN 50128
EN 50126-1 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process [8]	Observance of the processes according to EN 50126 – 1
EN 50126-2 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety [9]	Observance of the processes according to EN 50126 – 2

Note: Further legislation aspects must be analysed and defined country-specific

3.4. Impacts from further Regulations

Note: Impacts from further regulations must be analysed and defined country-specific

3.5. Assumptions and Justifications

4. Open points / issues

Nr.	Title	Description	Reference
1.	Processing of hand-shake (not home AT)	Processing of Handshake request (HSReq) by ATO-OB to an AT, that is not the “home AT” or “default AT” and preconfigured in ATO-OB	
2.	Mapping of SCI-OP	Verification of mapping of interface SCI-OP data and Subset-126 data [2] must be performed. In case of missing data, the interface SCI-OP must be modified.	
3.	Mapping of X2Rail-131	Verification of mapping of interface X2Rail-131 data and Subset-126 data [2] must be performed. In case of missing data, the interface X2Rail-131 must be modified.	
4.	JP deletion indication AE to AT	The JP split between several SubSys AT instances is performed on SubSys AE level. This requires a functionality to manage the deletion of JPs from a dedicated SubSys AT instance, if after an OP update the SubSys AT instance is not responsible anymore, but it still stores the JP part from the previous OP. This includes a JP deletion message from SubSys AE to SubSys AT. The functionality is integrated in the function ATO-SubSysUC1-AE-9	
5.	Train Capability Report	It is to be evaluated and to be decided, whether and how the function and interface communication of the Train Capability Report is to be implemented. In the following chapter 4.1 the information defined are documented.	Chapter 4.1

4.1. Open point ID5 Train Capability Report

4.1.1. SubSysUC5 Handle Train Capability Report

The SubSysUC5 Handle *Train Capability Report* is part of the open points list, ID5.

4.1.1.1. Subsystem Use case Goal

The goal of SubSysUC5 to provide functions to receive and to transform Train Capability Report information of an ATO-OB via SubSys AT and to provide this information as Train Unit Report to PAS.

4.1.1.2. Functional process flow

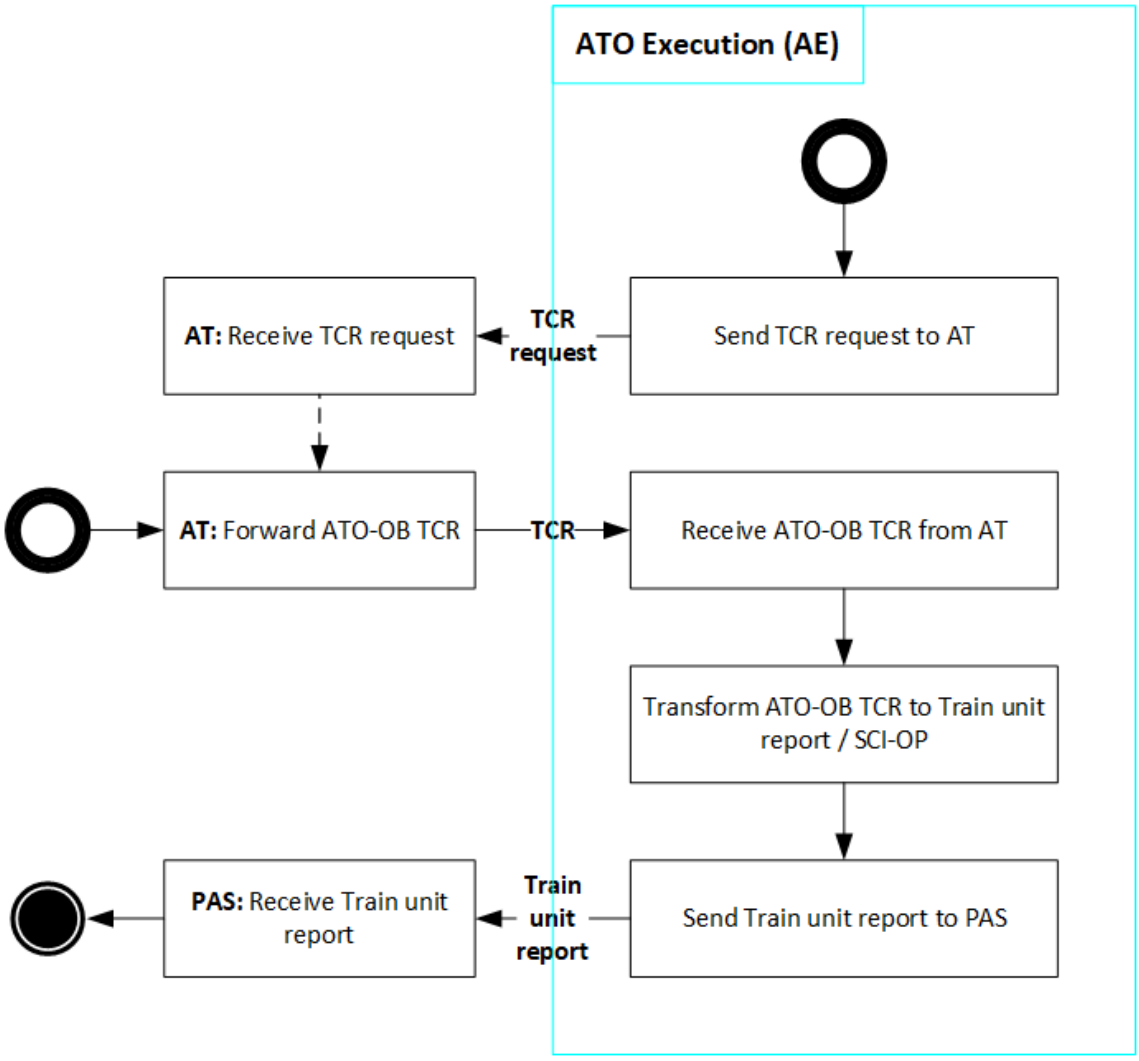

Figure 9: Process flow of SubSysUC5 Handle Train Capability Report

4.1.1.3. Exported constraints / requirements

In relation to the functional process flow of SubSysUC5 *Handle Train Capability Report* exported constraints and requirements as listed in Table 10must be considered:

Table 10: SubSysUC5 – exported constraints / requirements

ID	System	Description
SubSysUC5-EXCR-18	ATO-OB/AT	SubSys ATO-OB and SubSys AT shall process the TCR data
SubSysUC5-EXCR-19	ATO-OB/AT	SubSys ATO-OB and SubSys AT shall process TCR request and TCR session management
SubSysUC5-EXCR-21	SCI-OP	Interface SCI-OP shall implement a new message Train Unit Report to transmit TCR data of the related TCR and ATO communication session

4.1.2. High-level processual system functions SubSysUC5 TCR

In the following Table 11 the processual system functions of SubSys AE for the SubSysUC5 TCR, identified within the functional process flows per subsystem Use case are described on a high-level. The description is only meant to provide an indication and no detail design. The detailing must be performed in the subsequent development phases.

Table 11: High-level description of system function SubSysUC5 TCR

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC5-AE-78	SubSysUC5	Send TCR request to AT	SubSys AE sends the TCR request to AT. The TCR request might have the following differentiation: 1. Request to re-send a TCR report for an existing TCR communication session 2. Request to establish a TCR communication session 3. Request to disable an existing TCR communication session The differentiation might be implemented by different variable setting within the TCR request message. SubSys AT must manage the specific TCR communication session accordingly. Rational to implement a TCR request message: 1. The TCR request enables the system to request a TCR, when deviations of the train capabilities are detected by monitoring the operational plan. Due to the event driven TCR sending regime of ATO-OB, it might happen that ATO-OB is sending no TCR for a longer time, even if changes in the capabilities took place. 2. The TCR request enables the system to terminate the TCR communication session. 3. The TCR request enables the system to request the set-up of a TCR communication session.	X2Rail-131	TCR request

FCT-ID	SubSysUCID	Function Title	Description	Interface	Message
ATO-SubSysUC5-AE-42	SubSysUC5	Receive ATO-OB Train Capability Report from AT	SubSys AE receives the ATO-OB Train Capability Report via SubSys AT related to the established TCR communication session.	X2Rail-131	ATO-OB Train Capability Report
ATO-SubSysUC5-AE-43	SubSysUC5	Transform ATO-OB Train Capability Report to SCI-OP	SubSys AE transforms the ATO-OB Train Capability Report to the SCI-OP data format, by mapping it to the Map Data and converts it to SCI-OP, Train Unit Report format. SubSys AE divides and allocates the ATO-OB Train Capability Report data to the different data formats of the SCI-OP interface, as Operational Plan Execution Report, Operational Plan Execution Forecast, Train unit report.		
ATO-SubSysUC5-AE-44	SubSysUC5	Send Train unit report to PAS	SubSys AE sends Train unit report to PAS	SCI-OP	Train unit report

4.1.3. High-level Interface Description SubSysUC5 TCR

In the following Table 12 the interface communications for the SubSysUC5 TCR identified within the functional process flows per subsystem Use case are listed. The listing is only meant to provide an indication and no detail design. The detailing must be performed in the subsequent development phases.

Under the “Status” an indication for the current definition status of the interface communication is provided. The status is to be understood as the following:

1. “Defined”, the message / data defined in the functional process flows is already defined within the scope of the related interface communication.
2. “Extent”, the message / data used in the functional process flows must be extended by the data defined in the functional process flows within the scope of the related interface communication.
3. “Evaluate”, the interface communication as already defined must be evaluated in detail. It is assumed, that an extension of the interface communication is highly likely.

In any case detail definition and evaluation must be performed in the subsequent development phases.

Table 12: High-level description of SubSys AE interfaces SubSysUC5 TCR

FCT-ID	SubSysUCID	Interface	Message	Start	Destination	Status
ATO-SubSysUC5-AE-78	SubSysUC5	X2Rail-131	TCR request	AE	AT	Extent
ATO-SubSysUC5-AT-79	SubSysUC5	X2Rail-131	TCR request	AE	AT	Extent
ATO-SubSysUC5-AT-41	SubSysUC5	X2Rail-131	ATO-OB Train Capability Report	AT	AE	Extent
ATO-SubSysUC5-AE-42	SubSysUC5	X2Rail-131	ATO-OB Train Capability Report	AT	AE	Extent

FCT-ID	SubSysUCID	Interface	Message	Start	Destina-tion	Status
ATO-SubSysUC5-AE-44	SubSysUC5	SCI-OP	Train unit report	AE	PAS	Evaluate
ATO-SubSysUC5-PAS-45	SubSysUC5	SCI-OP	Train unit report	AE	PAS	Evaluate

5. References

[1] Subset 125 ATO over ETCS – System Requirements Specification, Version 0.2.0, 24.03.2022

[2] Subset 126 ATO-OB / ATO-TS FFFIS Application Layer, Version 0.1.0, 16.03.2022

[3] Subset 130 ATO over ETCS – ATO-OB / ETCS-OB FFFIS Application Layer, Version 0.1.8, 02.11.2021

[4] X2Rail-131 Part of Deliverable D3.1 ATO-TS / TMS FIS, Version 0.1.0

[5] Intentionally deleted

[6] RCA.Doc.48, Realization of RCA Goals

[7] Intentionally deleted

[8] EN 50126-1 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process

[9] EN 50126-2 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety

[10] EN 50128 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

[11] TSI TAF/TAP

[12] RCA.Doc.4, RCA Glossary

[13] RCA.Doc.18, RCA Domain Knowledge Specification

[14] TS 50701: Railway applications - Cybersecurity (draft), 2021

[15] IEC 62443: Industrial Cyber Security

[16] DIN VDE V 0831-104: Electric signalling systems for railways, 2015

[17] RCA: (Cyber) Security Guideline, 2021

[18] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety

[19] 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

[20] RCA.Doc.54, Solution Concept: MAP, Baseline 0, Release 4

[21] RCA.Doc.35, System Definition - System Capability 87, Baseline 0, Release 4

[22] RCA.Doc.74, Concept SMI (not released yet)

[23] RCA.Doc.40, RCA Architecture Poster, Baseline 0, Release 4

[24] RCA.Doc.69, MAP Object Catalogue, Baseline 0, Release 4