# RCA

## Reference CCS Architecture

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

# ATO - Concept

Document id: RCA.Doc 72

## Table of contents

## List of Figures

## List of Tables

## Change history

| | | | |
|---|---|---|---|
| 0.1 | 2021.11.15 | Arvid Báärnhielm, Jens Nolte, Katherine Stowe | First draft created, including proposals for chapter names and descriptions. |
| 0.2 | 2022-01-19 | Arvid Báärnhielm, Jens Nolte, Katherine Stowe | Updated chapters 1.3 and 2 |
| 0.3 | 2022-04-12 | Arvid Báärnhielm, Katherine Stowe | Large update due to cluster discussions |
| 0.4 | 2022-05-24 | Arvid Báärnhielm, Katherine Stowe, Simon Heller | Update after internal review |
| 0.5 | 2022-08-11 | Katherine Stowe | Updated after ATO cluster review |
| 0.6 | 2022-09-28 | Arvid Báärnhielm, Richard Deacon | Update after RCA Cluster and RCA Core Group reviews |
| 1.0 | 2022-09-30 | ATO Cluster | Formal incrementation for official release for RCA BL1 R0 |

# 1. Introduction

## 1.1 Release Information

**Basic document information:**

RCA.Doc72

Category: B (Concept)

CENELEC Phase: 1

Version: 1.0

RCA Baseline set: BL1 R0

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 Purpose of the document

The objective of CENELEC Phase 1 [4] is to develop a sufficient understanding of the system to ensure a proper performance of all subsequent RAMS life cycle activities. The result of this development has been captured in this document.

RCA includes the ATO system in the overall CCS system architecture. This document outlines the concept for the ATO related elements in the RCA Architecture and identifies the scope, context and purpose of the system, adjacent systems and the operational environment. It also outlines the operational expectations of the system, including high-level PRAMSS considerations.

This document may also contain some preliminary detail to inform the system definition, required as per CENELEC Phase 2 [5].

## 1.4 Terms and Abbreviations

For terms and definitions refer to ATO Glossary [1] or the RCA Terms and Abstract Concepts [2].

## 2 Scope of ATO

The scope of the ATO referenced in the RCA includes the possibility to operate in Grade of Automation (GoA) 1, 2, 3 and 4. ATO technology is based on the ERTMS/ATO system as defined by S2R X2Rail-1 and X2Rail-4, and published by the European Union Agency for Railways. The ATO provides the control functions for train operation, including driving and train-based operational tasks. This system will be utilized by the railway operators to improve performance and by the railway undertakings to automate train management.

Note: the ETCS provides the Automatic Train Protection (ATP) to the entire vehicle, including the ATO. The ATP system is not within the scope of the ATO system, however it is required for ATO to function.

The ATO system involves two major components: onboard and trackside. These interface to a centralised Traffic Management System (TMS) that includes functionality to provide the ATO system with necessary operational data, the Train with capabilities to support ATO, and the ATP (part of the CCS Onboard, which is based on ETCS). ATO has been designed to work with ETCS in Level 1, 2 & 3 (note: it is expected that Level 2 and Level3 will be merged under the name Level R in the coming TSI update of 2022). The ATO system has access to centralised topology data as used by other RCA components. The interfaces to these adjacent systems are included in the scope of the ATO system.

Figure 1 shows the major components and interfaces in the ATO system:

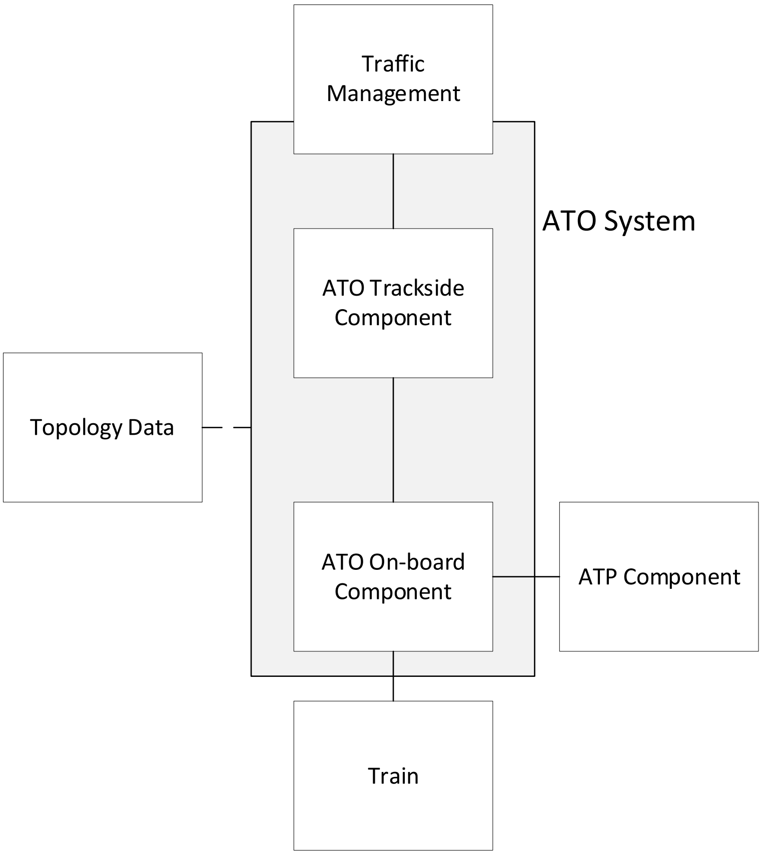
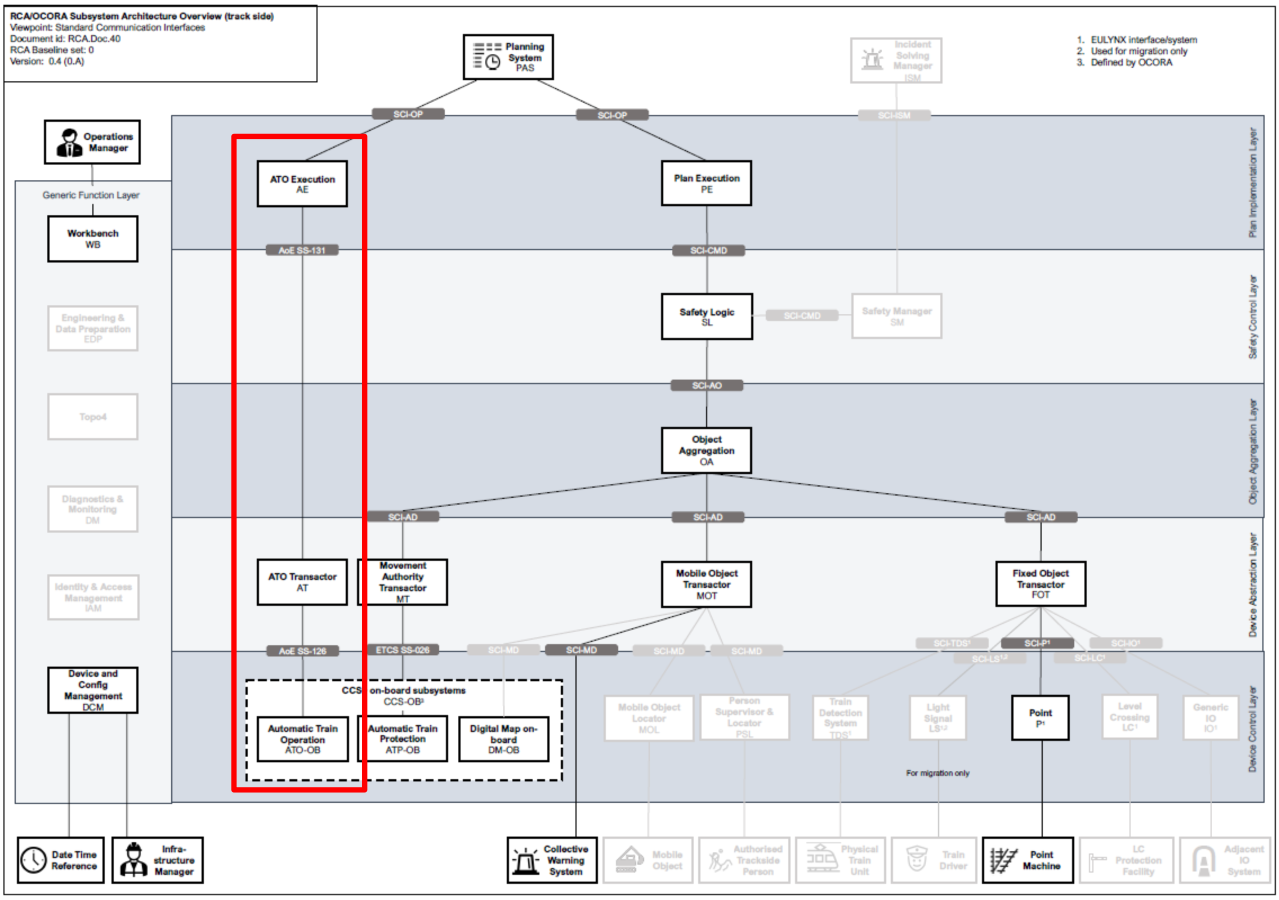


**Figure 1 - High-level system architecture**

Figure 2 below highlights the ATO relevant systems and interfaces in the RCA Logical Architecture [6]. Here the TMS has been separated into three components; the Planning System (PAS) (which is out of scope of the RCA), the ATO Execution (AE), and the Plan Execution (PE), with the AE and PE components located in the Plan Implementation Layer.

Note: Throughout this document, the PAS and AE will frequently be referred to as “Traffic Management” to connect to the high-level system architecture as shown in Figure 1.

The ATO trackside component, called the ATO Transactor (AT) interfaces to Traffic Management via the AE component which then interfaces to the PAS. The CCS Onboard system includes the ATO onboard functionality, alongside other onboard systems, such as the ATP-OB.



Note: Elements of light grey colour are not included in the modelling scope of RCA BL 0.4 release

Figure 2: The RCA Logical Architecture version 0.4 with the ATO relevant systems highlighted [6]

Note: The AE System Concept is defined in document RCA.Doc.73 [7].

# 3 Context of ATO

European Rail Traffic Management System (ERTMS) is a European-led initiative designed to provide a compatible train control system across Europe, which enables fitted trains to cross from one member state to another without technical restrictions as part of an interoperable railway.

ERTMS consists of two sub-systems; the European Train Control System (ETCS) which is an in-cab signalling system responsible for automatic train protection, and Global System Mobile - Railways (GSM-R) which is used for different types of communication in and around the train and railway track; this includes the communication necessary for ETCS to function.

Note: GSM-R is being replaced by the Future Railway Mobile Communications System (FRMCS), which is expected to be specified in the upcoming TSI release of 2022

ERTMS is mandated by Regulation through application of the Control Command Signalling Technical Specifications for Interoperability (CCS TSI).

The ERTMS/ATO system has been developed through EU funded research and innovation programmes. Firstly through the Trans-European Network Transport (TEN-T) project from 2012 to 2015 and subsequently through Shift2Rail which commenced in September 2016. The main European Railways and the major European signalling suppliers have worked collaboratively to develop the ERTMS/ATO system.

ATO specifications scoped to GoA 1 and 2, and an update to the ETCS specifications in support of ATO have been produced, see the relevant documents in Table 1 below. A test bench and pilot demonstration of the ERTMS/ATO system was undertaken within Shift2Rail to validate these specifications. GoA 3 and 4 specifications and validations are underway at the time of writing.

| Title | Reference | Type of document |
|---|---|---|
| ERTMS/ATO Operational Principles | 12E108 | Supportive |
| ERTMS/ATO Operational Requirements | 13E137 | Supportive |
| ERTMS/ATO Glossary | 13E154 | Supportive |
| ERTMS/ATO Operational Scenarios | 13E151 | Supportive |
| ERTMS/ATO System Requirements Specification | SUBSET-125 | Mandatory |
| ETCS-OB / ATO-OB FFFIS Application Layer | SUBSET-130 | Mandatory |
| ATO-OB / ATO-TS FFFIS Application Layer | SUBSET-126 | Mandatory |
| ATO-OB / ATO-TS FFFIS Transport and Security Layers | SUBSET-148 | Mandatory |
| ATO-OB / Rolling Stock FFFIS Application Layer | SUBSET-139 | Mandatory |
| ATO-OB Interface Specification Communication Layers for On-board Communication | SUBSET-143 | Mandatory |
| CCS Consist Network Communication Layers | SUBSET-147 | Mandatory |
| Application Guide for ERTMS/ATO | | Supportive |

| Title | Reference | Type of document |
|---|---|---|
| ATO-TS / TMS FIS | X2Rail-131 | Supportive |

Table 1: ATO relevant documents

The European Union Agency for Rail (ERA) have agreed that ATO shall form the 3rd sub-system of the ERTMS system and the specifications are therefore included in the CCS TSI 2022. The ATO sub-system is optional within the ERTMS system, as is the GoA level implemented, but if ATO is deployed it is mandatory to be compliant with the specifications in order to ensure interoperability across Europe.

# 4 Purpose of ATO

The primary purpose of the ATO system is to drive the train automatically so that it meets the timetable; the secondary purpose is to do this in the most energy efficient way. ATO displays more efficient, accurate and consistent driving behaviour than manual operation, resulting in a better-performing, high-capacity railway.”

The ATO system in the context of RCA must be modular to enable an interchangeable and interoperable system. This is so that European railways that adopt RCA will benefit from lower-cost signalling solutions.

# 5 Principles of ATO

As the ATO components within RCA reference the ERTMS/ATO specifications developed in Shift2Rail and included in the CCS TSI 2022, the Operational Principles [3] developed for this technology will also apply.

The development of ATO within RCA shall also pursue the following basic principles:

1. ***High-performing:*** The ATO system is able to operate the train, including driver responsibilities where applicable, more efficiently than current manual operations.
2. ***Safe:*** ATO functionality replacing safe functions performed by the driver shall be safe. ATO shall not impede on the safety of the ATP.
3. ***Migratable:*** It should be possible to migrate from existing ERTMS/ATO solutions (as defined in CCS TSI 2022) to the RCA ATO system without significant business impact. There should be a clear path to migration.
4. ***Modular:*** It shall be possible to implement any automation grade of ATO independently of other grades, or add/remove ATO functionality without affecting neighbouring systems.
5. ***Future proof:*** The developed solution shall be usable for the long term and be easily extendable.
6. ***Centralised:*** The ATO system shall use centralised topology, operational, signalling and train data.
7. ***Interoperable:*** ATO shall ensure interoperability across vendor solutions or infrastructure managers.
8. ***Reliable:*** The ATO system shall be reliable and able to support the availability needs of the user and minimize maintenance.
9. ***Energy efficient:*** ATO performance should be energy efficient wherever possible, and driving performance shall be able to be optimized.

# 6 Environment of ATO

## 6.1 ATO components located trackside

### 6.1.1 Physical issues

The ATO components AT and AE will be software-based functions that operate on a computer platform that may also be used for other CCS applications. This computing platform will be located in a trackside environment such as a railway operating centre. The building should provide space in a secure, temperature-stable environment where equipment can be accessed by operational and maintenance staff. ATO components are expected to interface to the existing diverse and secure power supplies with spare capacity to support critical systems. Consideration should be given to environmental sustainability in the design of heating and cooling.

Software-based systems located in this type of physical environment introduces cyber security and physical access risks. These trackside components are intended to be centralised for the railway network and therefore degradations to this centralised system could affect the ATO system.

### 6.1.2 System interface issues

ATO components will be accessible by people, including railway operators, via Traffic Management , and maintainers directly to the AT. Issues related to access authorisation and human factors need to be taken into consideration. Maintainers may interact with the system both remotely and directly, and require information to support both proactive and reactive maintenance.”

The AT will interface directly with Traffic Management via the AE component, and has a heavy reliance on this system providing timely and accurate data to support optimal running of the railway.

The influence of planning and operational decisions will impact the instruction sent by the AT to the onboard ATO component. The RU information that needs to be provided to the ATO onboard component to enable the operation of the train needs to be input to the system.

Note: The ATO system as defined today has been designed to work with any operational control system, from a simple static timetable up to a fully integrated TMS with dynamic timetable adjustment. The interface of the ATO GoA 2 trackside subsystem to a TMS has been defined through Shift2Rail [11], however is not mandatory as part of the CCS TSI 2022. The allocations of ATO related functionality between the RCA components AE and AT, clarification of the interfaces, and access to centralized databases is to be proposed.

The AT will interface to the ATO onboard component which is software-based functionality on an integrated CCS onboard computing platform.

## 6.2 ATO components located onboard

### 6.2.1 Physical issues

The ATO onboard component, ATO-OB, will be software-based functions that operate on a safe computing platform onboard the vehicle. As ATO functionality will be part of an integrated computing platform, hardware requirements will be driven by the requirements of all RCA components in the CCS onboard, which will consist of systems with a safety responsibility. The digitalisation of the vehicle resulting in an increased number of interconnected systems in the onboard system will introduce cyber security risks and heavy reliance on accurate and safe data and interfaces. The ATO will provide train control commands to traction/braking systems, and passenger door systems, which are of a mechanical nature and influenced by the track environment

### 6.2.2 System interface issues

Driver interaction with the ATO-OB will be via the ETCS DMI as outlined in the ERTMS/ATO specifications. Drivers will need to manage a larger amount of information from various digital systems. In addition to drivers, there will be other people interacting with and sending commands to the train, including from remote trackside locations.

The ATO-OB will interface with the ATP-OB (CCS onboard) and the vehicle. In GoA 3 and 4 scenarios, the system will be fully responsible for the safe operation of the train, transferring the management of the risks from the human to an automated, computer-based system.

The train will be operating in an unpredictable railway environment and therefore all functionality allocated to a driver must be allocated to the ATO for GoA 3 and 4. This includes the reliable detection of objects on the line, responding to adjustments in planning and safe train movement permissions.

## 6.3 Legislative and economic issues

Mainline ATO technology has been standardised across Europe, and railways are legally obliged to comply with the CCS TSI. Modifications and enhancements to ATO technology needs to be managed through ERA.

The homologation of ATO products, is required, especially for GoA 3 and 4, where there is no driver present.

The ownership of the data needed for the ATO operation could introduce challenges as it needs to be transferred and shared between the different organisations (e.g. RUs and IMs).

Many railways in Europe are facing financial challenges. There is an economic driver behind the modularisation of CCS technology, including ATO, as this enables an open market and greater competition within the supply chain.

# 7 PRAMSS and performance requirements

This section provides an insight the PRAMSS and Non-Functional Requirements (NFR) that shall be considered throughout initial system development phases.

## 7.1 Performance

The ATO system should operate the train more efficiently and accurately than current manual operations, driving in a way that conserves energy (wherever possible), reduces wear and tear, and improves capacity. The ATO will be responsible for performing various driver responsibilities, such as pantograph management or door management. These operations should be performed by the ATO system more reliably and with a faster response time than a manual operator.

Additionally, the ATO must be able to maintain as high a performance level as possible during minor degradations to infrastructure, for example, managing power consumption in high-demand scenarios, or driving within Temporary Speed Restrictions.

## 7.2 Reliability

The ATO System accuracy needs to be highly reliable, particularly in GoA 3 and 4, where operators require the system to operate as intended as there may be no possibility for intervention via the trackside. Additionally, failures need to cause as little disruption as possible, and all degraded scenarios should be understood and a recovery process in place for each.

## 7.3 Availability

Performance improvements can form a key part of a railway’s business case and therefore in most cases a high availability is expected of the ATO system. For GoA 3 and 4, where there is no or little manual intervention possible in case of system failure, redundant systems and processes needs to be put in place.

System availability depends on hardware and software availability which will be covered by overall RCA RAM analysis. For a reliable system, security requirements become key in supporting high-availability.

## 7.4 Maintainability

A reliable system should reduce the required maintenance. Maintenance and updates to ATO software need to be done remotely and automatically where appropriate. This improves system availability, and the safety of the system due to a reduced need for maintainers to access onboard components that may be located on the live railway. Remote access is particularly important for GoA 3 and 4 where the ATO system is responsible for interrogating and reacting to faults during normal operation.

Useful, timely and reliable diagnostics capabilities become important to support ATO components in the RCA, and diagnostics and maintenance data should be standardised and provided to a centralised location in real time, to aid in rapid maintenance response and to avoid the need for bespoke maintainer knowledge.

## 7.5 Safety

### 7.5.1 GoA 1 and 2

GoA 1 and 2 does not introduce any safety requirements on to the ATO system as all safe train operation functions are divided between the ATP or the driver. However, some safety-related functionality that was previously the role of a driver still requires management by the ATO system, this includes adjusting driving styles for low adhesion conditions, hill starts and managing infrastructure that may impose strain on freight couplings.

### 7.5.2 GoA 3 and 4

GoA 3 and 4 functionality introduces additional safety requirements on to the ATO onboard system, for example the identification and safe reaction to objects on the line, and responding to onboard emergencies. These functions should meet a high safety standard and mitigations to safety risks such as redundancy, remote observation and diagnostics, remote driving intervention need to be included in the system.

ATO driving and stopping functionality will still utilise the ATP system to ensure overall safe operation and movement of the vehicle, which may result in exported requirements on to this system to support the ATO operational scenarios, particularly where GoA3 and 4 introduces many new safety-related functions.

It is the intention that the safety requirements imposed on the ATO trackside components are as low as possible, as the CCS onboard (including the ATO onboard component ATO-OB) will execute the plan and ensure safe movement and operations.

### 7.5.3 Data assurance

The ATO relies on safe data, including but not limited to: train data, sensors that perform supervision tasks such as observing the clear track ahead and train, signalling status and topology data. The assurance of dynamic, real-time data should be automated, and centralised to maintain a “single source of truth” for all safety related data.

For more detail on data see Section 9.

## 7.6 Security

As RCA components can be executed on connected computing platforms, additional cyber security risks may be introduced. Protecting the system from security threats is unlikely to impact the safe operation of trains as this is protected by the ATP, however as the ATO does perform some safety related functions and relies on remotely transmitted data, it still needs to be protected from malicious attacks. Additionally, ATO should focus on security requirements that support high availability of the system.

# 8 Regulation analysis

This chapter identifies the relevant regulations, laws and norms that must be considered, or may be impacted by ATO developments in the RCA.

## 8.1 Interoperability

It is critical that the onboard and trackside functionalities are clearly allocated and there is a clear single interface between these two components to support interoperability across Europe. This can be guaranteed by the use of the Shift2Rail ERTMS/ATO specifications which consider interoperability a core principle of the design.

With the new 4th Railway Package, the rail regulation has had important changes. Interoperability regulations are the most important ones. Main legal documents that affect the train control and command systems are:

- Regulation (EU) 2016/796 on the European Union Agency for Railways. Describes the responsibilities of the European Rail Agency for system approval.
- Directive (EU) 2016/797 on the interoperability of the rail system within the European Union: describes the systems and subsystems to ensure the interoperability throughout Europe.
- Directive (EU) 2016/798 on railway safety: as its name suggests, stablishes the legal framework to perform risk evaluation processes, monitoring activities and safety assessments.

From these regulations a set of Technical Specification for Interoperability are born. Each TSI describes and specifies the rail system or subsystem to guarantee interoperability.

## 8.2 Safety legislation/standards

According to the European directive 2016/798, compliance with the safety requirements shall be demonstrated to ensure the safe integration into the railway system and respect of the safety objectives when in service (for example, to achieve allocated THR's for the localisation functions). In this context and following the Common Safety Methods (CSM) is allowed to apply the CENELEC standards. For the rail domain the following standards apply:

- EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process, CENELEC [4]
- EN 50126-2, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety, CENELEC [5]
- EN 50128 Railway applications - Communication, signalling and processing systems. Software for railway control and protection systems [8]
- EN 50129 Railway applications - Communication, signalling and processing systems. Safety related electronic systems for signalling [9]
- EN 50159 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems [10]

## 8.3 Harmonization of safety requirements

As a part of the safety analysis, the following systems may be affected:

- The CCS onboard: The safety protection functions required to support ATO operations in GoA 3 and 4 may need to be managed by the ATP.
- The vehicle: the integration of sensors into the vehicle to support supervision functions.
- The PAS: The provision of planning information supporting ATO, including missions, timings, train consists, etc.
- Topology/map databases: The provision of data with an accuracy that supports high ATO performance.

# 9 Data

## 9.1 Topology/map Data

A centralised source of topology data should be used for the ATO system. The centralised topology database that crosscuts the RCA should be viewed as the source of truth for track description data, which should be aligned with the Digital Map onboard and made available to the ATO-OB during operation. This will be a change from the current ERTMS/ATO specification which uses track description data provided by the ATO trackside in the form of a Segment Profile.

Alignment of the centralised topology data base is needed to ensure ATO requirements are met, and this data base should be safe, secure, highly available and assurance of data should be automated where possible due to the dynamic nature of the information.

## 9.2 Train Data

The ATO system requires train data so that it can accurately control train operations. A single source of train data should be used by the ATO system, sharing data automatically to eliminate the need for driver or operator input. Fundamental train data should be provided by the vehicle, to avoid the management of train information on the trackside, whereas train configuration information will be provided through the interoperable interface between Traffic Management and business operations systems.

## 9.3 Planning and Operational Data

There are two types of operational data provided to the train to support ATO, mission and journey information. Dynamic adjustments may be made to train operations, as informed by traffic management system, and the ATO should be capable of managing dynamic data.

As the ATO will be constrained by the behaviour of the ATP, signalling layouts need to consider ATO behaviour to ensure compatibility between End of Movement Permission locations and timing points, and that track layouts support the higher capacity possible with ATO.

ATO performance is limited by the arrival times contained in journey information. Planning should consider the higher performance possible by an ATO system to maximise the capability of the ATO system.

# 10 Exported requirements

None identified at this time.

# 11 Tensions, Assumptions & Justifications

## 11.1 Tensions

- It should be reviewed whether the AE and PE should become a merged component as the value of modularity of the ATO and Planning functionality is not clear. The AE currently has its own Concept Document [7].
- The ATO onboard components need to be aligned with the developments related to the CCS onboard such as OCORA and Digital Map.
- Some ATO onboard functionality may be better allocated to the ATP system, a coordinated development of the ATO and enhanced ATP functionality should be undertaken.
- The investments made by railways and suppliers into the ATO/ETCS specifications developed within Shift2Rail should be preserved where possible in the development of RCA.

# 12 References

The following documents provide related references:

[1] 13E154, ERTMS/ATO Glossary, v1.11, EUG

[2] RCA.Doc.14, RCA Terms and Abstract Concepts

[3] 12E108, ERTMS/ATO Operational Principles, v1.8, EUG

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

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

[6] RCA.Doc.40, RCA Architecture Poster – Preliminary Issue with OCORA contribution, Version 0.4 (0.A), 26/04/2022, EUG and EULYNX partners

[7] RCA.Doc.73, Concept ATO Execution

[8] EN 50128 Railway applications - Communication, signalling and processing systems. Software for railway control and protection systems

[9] EN 50129 Railway applications - Communication, signalling and processing systems. Safety related electronic systems for signalling

[10] EN 50159 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[11] X2Rail-131, ATO-TS / TMS FIS