RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

APS Concept

Document id: RCA.Doc.51

Table of contents

List of Figures

List of Tables

Version history

Version	Date	Author	Description
0.1	2021-09-09	Martin Kaufmann	Initial draft
0.2	2021-11-29	Bettina Morman, Martin Kaufmann, Frank Schiffmann	Draft for internal review
0.3	2021-12-21	Bettina Morman, Martin Kaufmann, Frank Schiffmann	Updated according to review results
0.4	2022-03-18	Bettina Morman	Updated according to review APS cluster
0.5	2022-07-28	Bettina Morman	Minor updates to align with APS detailed concepts
1.0	2022-09-30	Frank Schiffmann, Bettina Morman	Version for RCA BL1 R0

Executive Summary

Interlocking systems have evolved historically which leads to today's **vast system and product landscape** that tries to mitigate the growing demands for route protection. Every introduction of a new or additional signalling and train control systems, such as the European Train Control System (ETCS), required **additional project engineering configuration and implementation efforts**. This is partially due to the fact that existing engineering and configuration data could not be reused because of a lack of compatibility or their inexistence (except as configuration in one interlocking system). Therefore, dependency in between life cycles is extraordinarily high in today's railway infrastructure and is a **major cost driver** for railway Infrastructure Managers.

The Advanced Protection System (**APS**) is a set of essential core functionalities of the **R**eference **CCS A**rchitecture **RCA**. It enables a very strong simplification of the future CCS architecture and a very precise and safe control of traffic through higher-level traffic management systems and a highly efficient migration from the current system landscape towards the RCA system architecture. Therefore, APS will be realised on a **computing environment and a communication network** interfacing with different parts of RCA and external entities.

APS always controls the granting of a safe movement path for a train, based on a **fail safe and unified topology representation**. This is possible due to the purely geometric determination and safety check of a movement path for a train which is based on the **abstraction** of route elements into a geometric extent.

APS does not delegate any safety requirements or safety-related application condition to processes or other systems regarding to the track usage. All operational decision-making and traffic flow optimisation functionality will be delegated to the Traffic Management System. Hence, APS does not make any **operational decisions and optimisations** but performs **generic safety checks** that are applicable to any topology. Therefore, APS consists of a generic set of functions based on **harmonised operation** considering abstracted information and clear distinction between operational and safety functions. Thus, APS needs to be interfaced to a system that manages the operational level which is called Plan Execution.

APS receives requests from Plan Execution for protecting the running path of a train or state change requests for trackside assets based on the needs of the Traffic Management System. Every received request and **occupancy claim** of a certain segment of the topology is represented in the **operating state**. APS performs safety checks in order to either grant or reject the request, considering the current operating state. Also **Warning Areas** to protect track workers and to enable construction and maintenance as well as **Usage Restriction Areas** for handling further operational reductions are saved into the operating state

APS checks if the state change request for trackside assets can be executed safely and if so, sends a state change demand to the corresponding **Object Controller** interfacing to the various switchable elements in the field. In order to be able to perform safety checks, APS uses **safe location information** of trains equipped with a **Radio communication system** (and other sources) in the appropriate form and format (e.g. Positioning Report for trains equipped with ETCS). Thus, APS translates and sends a granted request for a secured running path, which is called **Movement Permission**, to the specific track-bound train unit.

APS can also interface with legacy applications allowing the **safe transition** to areas that are not equipped with APS which directly opens the door to many possible **migration strategies**.

In addition to the main functionalities, APS also considers various **degraded situations** (e.g. loss of location information) and how to handle them.

The concept of APS introduced in this document enables the creation of **standardised interfaces in a modular architecture** which highly reduce today's maintenance effort and increases track worker safety. APS allows different **configurations** which require significantly less planning and engineering based on the generic approach of the safety logic. Hence, also a much **faster safety approval** on the market and authorisation into service is possible. APS enables an overall **automation** of the rail operation and various processes in the product life cycle (development, integration, operation) due to the high degree of modularity and standardisation.

1 Introduction

1.1 Release information

Basic document information:

RCA-Document Number: RCA.Doc.51
Document Name: APS 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 Disclaimer

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. 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 this document

This document is based on reference document [2] and documents APS main System Requirements. All references can be found in chapter 1.5.

In addition, this document shall show proposed solution approaches to overcome existing challenges and shall give a first insight into the differences between APS and today's legacy trackside signalling solutions like interlocking. Therefore, the document shall be treated by reading as very first draft.

1.5 Scope

The Advanced Protection System (APS) is a core element of RCA, which in turn is generating an architecture description (business and operational requirements, and interface specifications) to be used as a **standard reference tender specification** for enabling of further specification steps and specific implementations.

This document is part of a set of documents that will form the overall "A.P.M. -concept". Other documents of the APS concept describe operational scenarios, system definition and analysis, or functional analysis and logical architecture.

Currently the "A.P.M concept" as well as this document are work in progress.

The document will be updated periodically to line up with additional upcoming concepts for several parts of RCA.

APS is located in the middle of the CCS trackside architecture, which has the typical form of an "industrial automation pyramid".

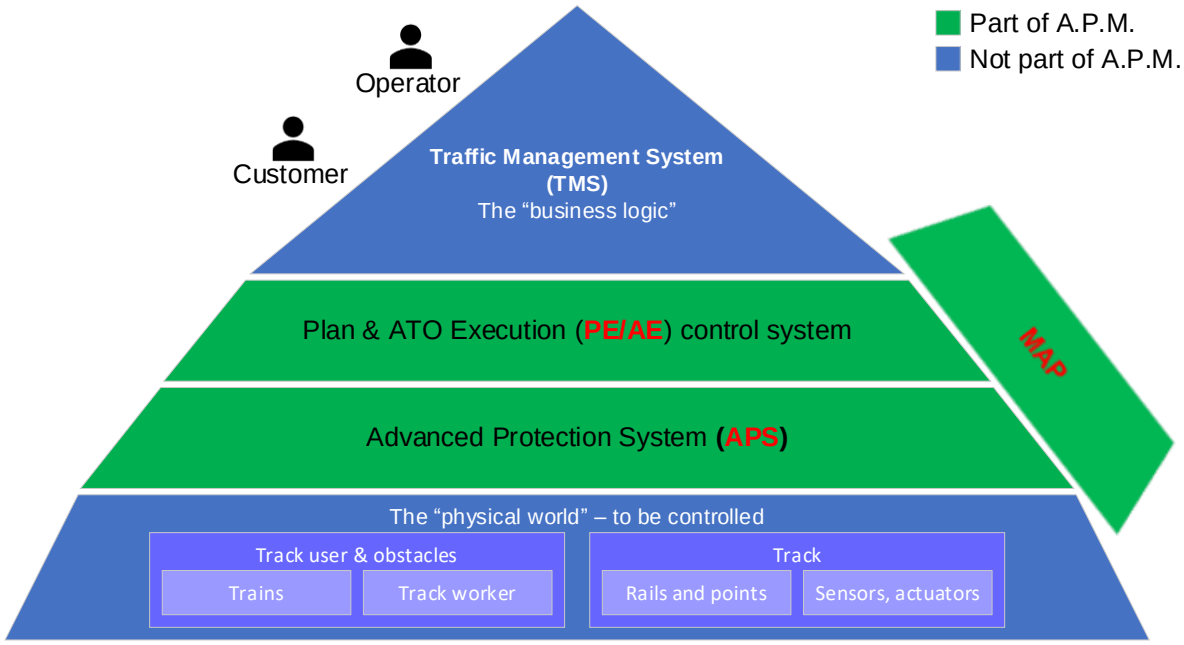

Figure 1: APS in context of the railway production

The Traffic Management System (TMS) plans and decides "when and what to do". The Traffic Management System continuously (re-)plans the timetable and decides about measures to optimise the flow of traffic on the network. TMS is typically a large IT system landscape which delivers a production plan (see Operational Plan in [6]). The production plan formed by the Traffic Management System is analysed and executed by "plan execution" control systems. The subsystem ATO execution (AE) translates the operational plan into ATO-specific demands and the subsystem Plan execution (PE) forms the discrete requests for securing the running path.

"Plan Execution" (PE), "Advanced Protection System" (APS) and "Map" are core subsystems inside RCA and are referred to as "**A.P.M.**" in this document: "**A**dvanced protection system, **P**lan execution and **M**ap data management".

The APS assures as a gatekeeper specialised on safe functions so that the plans and requests of the TMS and AE/PE create a safe traffic flow and then executes them. APS assures safe track usage and uses the information provided by on-board equipment of trains, mobile track user devices (maintenance teams) or track-side assets to control and supervise the railway production. APS must fulfil very high availability, safety and security standards as well as performance demands.

APS is a generic form for functions of the future railway system architecture that are today located for example in Interlocking (IXL), Radio Block Centre (RBC) and trackside functions needed for controlling automated train operations. Or in other terms: APS is the trackside Command-Control and Signalling (CCS) subsystem in RCA, excluding TMS, PE or the switchable field elements including legacy and future train detection systems.

APS does not stand for a certain technology; it stands for a set of **challenging business targets** and requirements. The concept of APS and its principals introduced in this document give a first impression of the innovation possible in this area.

1.5.1 Scope within RCA

The Advanced Protection System (APS) is part of the proposed RCA set of building blocks and forms an essential proportion of the trackside CCS subsystem in RCA covering the defined enhanced CCS+ system in scope of development a next generation of CCS within Europe's Rail Joint Undertaking Master Plan.

This set of building blocks will allow to build CCS trackside applications interfacing to additional Traffic Management applications including continuous monitoring. Traffic Management Systems interface via Plan Execution (PE) that is part of the proposed scope of RCA.

Note: The RCA is a proposed Architecture. In this document, the focus lies on covering objectives with basic requirements and proposals for solution approaches to cover the identified basic requirements.

Note: Currently several terms are used for describing the building blocks. The terms components or subsystems (as symbolising a part of a system) are used. If these are used, they shall be understood at the moment similar for describing something to be nominated as a potential product. If subsystem is used in the defined term for the CCS subsystem defined in the TSI CCS, this is elaborated accordingly.

APS interfaces the switchable Field Elements via EULYNX-compliant interfaces for enabling the possibility of handling existing installations. A rollout with compliant Object Controllers is a prerequisite for an APS introduction. In addition, APS is able to process localisation information independent of the specific underlying localisation technology by using standard interfaces.

The onboard part is handled by the standardisation initiative OCORA, covering the CCS onboard installation. Automatic Train Operation (ATO) is also part of RCA enabling the usage of given permissions by APS in an automated operation. Both, APS and ATO interface the trackside and onboard subsystem via UNISIG-standards.

A major enabler for the proposed architecture approach is the provisioning and use of a generic Basic Network Topology approach (MAP), supporting all trackside applications with a single data source and generic object abstraction as described in chapter 2.1. Note, that in current RCA architecture document [3] the term Topo4 is used, but different than MAP. Topo4 gives only the data preparation and MAP intention is to publish information. Not all candidates are given in the architecture yet, for handling all the MAP parts. But, for the meantime the terms Topo4 and MAP can be used similar for overall mentioning the data.

1.5.2 Out of Scope

The following functionalities shall not be supported by APS:

- Operational dead-lock prevention
- Automatic train routing and dispatching
- Safety validations of Object Controllers (OC) and localisation systems like for example:
    - recording of performance, diagnostics, and safety-related information of OC system conditions
    - setting of any system conditions with a secure fault release
    - Safe data aggregation and transmission to APS of information on detection of the position of train units and authorised staff including the correct identification and safe handling of position accuracy

The following functionality must be provided outside of APS for ensuring a safe rail operation:

- The functionality of safely controlling accelerating and braking of train units shall be provided by the onboard Train Control system.
- Correct forming of train compositions including the provisioning of safe train characteristics and data.

1.6 Use of This Document

The APS concept documentation shall be used as a general description that helps to understand the basic intentions behind the APS. It will be used for communication and onboarding events, for discussions about product development strategies, or to describe the business expectations for feasibility studies or for the design of prototype projects and pilot lines.

Please consider the referenced documents for deeper understanding of the business targets and objectives referenced in this document. The leading “@-symbol” indicates an objective and the leading “$-symbol” tags a system requirement. Each @objective will be addressed with one or multiple system requirements, later

referred to as $system requirement. All $system requirements are listed in to give an overview of all APS main requirements.

1.7 Target Group

The target group for this document are asset managers, product managers, system architects, designer of operational processes, system engineers and industry representatives.

1.8 Related Documents

Reference ID	Document Title	Source ID	Version
[1]	A.P.M. Business strategy, targets and problem definition	RCA.Doc.50	0.6
[2]	A.P.M. @Objectives	RCA.Doc.53	0.6
[3]	RCA System Architecture	RCA.Doc.35	0.3
[4]	RCA Terms and Abstract Concepts	RCA.Doc.14	1.0
[5]	Concept: MAP (Overall Solution Concept)	RCA.Doc.54	0.3
[6]	Concept: SCI-OP (Standard Communication Interface Operational Plan)	RCA.Doc.31	1.1

1.9 Terms and Abbreviations

For terms and definitions refer to the RCA glossary [4].

1.10 Structure of this Document

As input for the APS Concept, the A.P.M. business targets [1] were evaluated regarding their relevance for APS in [2] resulting in derived objectives for APS. Annex A: List of objectives gives an overview of the objectives relevant for APS and groups them into categories. Each category corresponds to a subchapter in chapters 3 and 4.

In addition, four core principals of APS are taken into account and mentioned in the relevant chapters of the document. These are derived as highlighted statements based on the business targets and the spread objectives relevant for APS:

- Core Principle 1 – Deploy a unified railway network topology data representation
- Core Principle 2 – Represent Current operating state
- Core Principle 3 – No operational and processual functionality
- Core Principle 4 – Deploy Generic Safety Checks

The structure of the document is following this approach:

Chapter 2 of this document introduces a few important prerequisites that enable APS.

The subchapters of 2, 3 and 4 are structured in the following way:

1. Objectives and System Requirements (chapters 3 and 4)
   The fulfilment of the objects through derived system requirements (requirement tracing) will be demonstrated at the beginning of each chapter in a table (see below). The focus of chapter 3 lays on non-functional system requirements whereas chapter 4 focuses on functional system requirements

Objective	Requirement

2. Problem description
   Description of the problem with today's interlocking.
3. Solution approach
   Description of the solution approach to the problem.
4. Migration (only chapter 4)
   Short overview of possible migration scenarios.
5. Degraded Modes (only chapter 4)
   Examples of relevant degraded modes for further analysis in a later development stage.
6. Delta
   Brief conclusion of the previous subchapters highlighting the main advantage of APS.

2 Prerequisites to enable APS

2.1 Fail Safe and Unified Topology Representation

2.1.1 Problem description

Nowadays, legacy systems typically use their own representations and formats to describe the track topology and possible objects e.g., a train path on the railway network. The information used by one system differs from data of other systems. Communication in between systems is either not existent or requires high efforts in mapping the different representations and to keep them up to date during the life cycle of the systems involved. Simple and standardised interfaces are not existing including the absence of a standardisable translation base for all the proprietary topologies and object representation description languages.

This leads to:

- High efforts for updating information in various systems, e.g. in case of changes to be applied based on this information silo principle
- High efforts to create interfaces for each application
- Problems for introducing a wider data exchange between different Infrastructure Managers and Railway Undertakings like it is foreseen in the European Railway referenced on the achievements of the 4th Railway Packages with an optimal data exchange
- Huge mismatches between documented application and real existing ones in the field
- Certain risk for unsafe situations when implementation conditions are violated
- Safety-issues in the overall railway system concerning wrong data without any clear responsibility for resolving

It can be summarised as a lack of a uniform standardised and safe topological representation. The APS concept doesn't work with proprietary topology description languages. A unified description language is needed.

2.1.2 Solution approach

The standardisation of a common reference frame for the logical representation of the railway network topology enables all consumers (aka systems, components) the following:

- Unified definitions
- Exclusion of false interpretations
- Uniform versioning
- Clearly defined handling of version changes
- No exclusion of specific applications

Such a common data basis for a logical railway network topology representation is called “Map data”. It integrates the safe part of the topology on a “fail safe topology” approach. This prerequisite is one of the core principles of APS and detailed in the following part.

Core Principle 1 – Deploy a unified railway network topology data representation

To be able to interface many different subsystems within RCA (and potentially beyond) with minimal interdependency, an important core principle is a unified logical abstract representation of the railway network and all its current characteristics and states. This abstraction comprises:

- The railway network within the Area of Control of an APS
- Occupancy claims regardless the technology used for localisation (e.g., trackside train detection system, GNSS, cameras) and operational reason (e.g. track work areas, movements)
- Switchable Field Elements used for securing of the route path of the train unit including additional risk mitigation measures like flank protection if needed
- Track sections that are not to be used at the same time (undercutting the minimum structure gauge of the infrastructure and reference profile of the train unit)

By abstract object representation realised on a unified topology data representation, it becomes possible to define every physical object interacting on a railway network geometrically. Thus, the way is paved for

- Using a minimal set of generic safety functions to cover all safety functionality required (see chapter 3.1)
- The simplification and standardisation of interfacing various switchable Field Elements or localisation technologies with no or very little interdependencies (see chapter 3.2)
- Replacing and/or removing existing equipment like localisation technologies step by step without changing the safety logic of APS or without a hug effort for project planning and design (see chapter 3.4)
- Separation of components with different life cycles (see chapter 3.5)

For reaching these targets, a generic and abstract representation of the railway network topology is a major enabler.

The railway network consists of a set of track axes. A track axis - the centre line between the upper edges of the rails - is a logical entity. However, due to its simple derivation from the physically existing rails, it has a very concrete reference to reality. It is basically a linear structure.

Track axes are described by their geometry. The geometry contains both the shape (curvature and gradient) and the position (coordinates) and is represented as a sequence of alignment elements.

For operational purposes, navigability on the entire railway network topology is the central requirement. As far as geometric information is concerned, the length of the track axes is for many APS use cases sufficient. From the geometric information, it could be calculated where several common axes meet and thus where branching points are located in the topology. However, this would be time-consuming, and the results were identical as long as the physical railway network topology does not change. Therefore, the Map Data shall be defined as an abstract view of the railway network topology. This data combines sequentially consecutive track elements into edges and sets nodes in the branch points. This view of the railway network topology is suitable for statements on navigation on the topology defining the physically possible travel direction from one Edge to another Edge via adjacent Nodes.

In the interaction between topology and geometry, the topological edge is the independent object. The 1 to n alignment elements that describe the geometric course of the edge reference the edge and are thus the dependent objects.

Each Node represents either

- Physical branching possibility of a track route (e.g. a single point) or
- A physical end of a track (e.g. buffer stop) or
- An operational borderline on a track ("responsibility border" between two adjacent systems like APS or the specific locations for legacy interlocking and RBC).

Note: A track intersection is not represented as Node (may be represented as separate entity in order to represent an intersection).

Each Edge has a

- Technical direction (from Node, to Node)
- Length in order to position and logical representations of physical track side elements or specific spot locations in the model (e.g. a speed change marker would reference a specific edge on position 123 on this edge and in the direction of this edge). Possible convention: 0 Meter at the position FROM Node, x Meter at the position TO Node (x>= 0 Meter)

At least the following field elements shall be logically represented in the topology data:

- Field elements that influence a movement direction of train units such as point blades
- Field elements that allow or hinder a passaging for train units such as a lifting bridge or a gate
- Field elements that protect a movement of a train unit such as level crossings and derailers

- Edges or edge sections with insufficient minimum clearance in order to avoid flank and stray collisions (e.g. multiple rail track, track sections between point heart and boundary marker) shall be logically represented on this Node-Edge Model

Note: Further subsystem specific objects such as information about track conditions (e.g. speed profiles, superelevation, gradients, curvature) shall be represented as linear objects.

In addition to the need of a Node-Edge Model, each information must be generated in a safe way. Safe means, that the information is correct from any safety consideration. This can be accomplished if the information fit to the present situation and if in case of information abstraction, e.g. by rounding, this is performed to the safe side considering the application dealing with the information.

While enabling this, APS will get a fail-safe topology representation.

2.1.3 Delta

Compared to today's interlocking and signalling systems, within RCA mutual 'Basic Track Topology Data' shall be used in order to allow a communication between all parts of RCA without the need for translation and/or interpretation. APS will use the same topology reference data source and the same version of a topology data set as all interfaced systems do. The topology reference data shall be based on a standardised model that represents the physical railway network topology in form of a logical Node-Edge Model, see [5].

Utilising the identical version of topology data among all involved parts of RCA allows:

- Common frame of reference
- Common interface language to describe, for example
    - routes along the railway network
    - spot location positions and geometrical extent (e.g. for track occupying elements, for positioning of trackside elements along the railway track)
- No or less room for interpretation and/or effort for implementation of translation between parts of RCA
- Same information content for all systems involved

Using common Map Data requires a form of common orchestration when changes occur. In contrast to today's highly manual processes for synchronising the topology data between the trackside parts of RCA involved shall be synchronised automatically (See chapter 3.6.3. The triggering should be possible manual, if needed,

Further on, (temporary) changes to topology capabilities such as for instance temporary speed restrictions or topology availabilities such as for instance temporary track closures are being communicated instantly among all consumers without the need for interpretation and without the disadvantage of not fitting to the current version of the Map Data.

2.2 Object Controller

2.2.1 Problem description

Nowadays, legacy systems use either a direct interface between switchable Field Elements and the interlocking system or use a proprietary Object Controller. This leads to the following problems:

- Fixed binding of the technical architecture to a proprietary solution with a high amount of collateral effort in case of changed and missing dependency between field elements and the interlocking, hindering any simple migration
- Missing exchange of control parts for switchable Field Elements due to missing usage of a standard control element (e.g. standardised Object Controller)
- Missing market for the development of a standardised Object Controller

- Missing possibility of migration of the signalling system independently from the version of the Object Controller and by reusing existing installations already equipped with Object Controllers

2.2.2 Solution approach

For enabling a simple interface of APS towards the level of the field elements, a standardised unified Object Controller from the perspective of APS must be present. Thus, independence from the functions and software versions in APS to the equipment installed in the field can be reached.

This goal can be enabled from the view of APS with:

- Standardised Object Controller interface towards APS
- Present Object Controller adapted for interfacing towards APS

An RCA-compliant Object Controller must be developed and available on the market to interface to APS if this variant shall be chosen. Object Controllers further need to be installed in the wiring when a signalling system will be migrated from legacy interlocking towards APS.

The development of the Object Controller and the interfaces must be performed in closed partnership with RCA. This focus topic is given under the responsibility of EULYNX.

The following two **Objectives** (see document [2]) are covered by these prerequisites:

- APS@Reuse existing field elements with object controller
- APS@Support EULYNX standards for interfacing with field elements via Object Controller

Any adaptions needed for avoiding a major change in the APS safety logic can be performed within the Object Controllers for recalculation of data enabling interfacing variants of outfield equipment as much as possible. This is implicitly required for the variant to existing Object Controllers.

2.2.3 Delta

The usage of a standard and the limitation of object controllers as a standard interface towards a generic system like APS is a fundamental change in the architecture, compared to existing interlocking environments. This is valid also for newly defined interlockings based on EULYNX, while early implementation projects use also proprietary Object Controller.

2.3 Plan Execution for interfacing to operational level

2.3.1 Problem description

Signalling systems are developed and constructed considering specific operational needs and operational processes of each Infrastructure Manager. This leads to a fixed relationship between operational level, including national Traffic Management Systems, and the level of interfaced interlockings as well. There are also big differences on the level of Traffic Management owned by different Infrastructure Managers. Some have very efficient and capable systems, others do not have a dedicated TMS at all but regulate operation manually by interacting with the interlocking system. This is possible due to operational rules being implemented in today's interlockings.

The lack of a clear split between operational level and signalling layer results in products, tailored to specific Infrastructure Managers operational requirements, that can be adapted for other railways with typically high development and engineering efforts. These isolated solutions are unfit for widespread application and cannot fulfil the needs of APS' lean safety logic and generic safety checks.

2.3.2 Solution approach

For interfacing APS as the core of the command-control and signalling trackside solution, a transfer system towards the specific operational usage must be present. This part is introduced as Plan Execution (PE) within the 'Reference CCS Architecture' defined in [3].

The presence of PE, including an associated operational harmonisation among all stakeholders (see chapter 2.4), is a fundamental base for APS.

Part of this coordination process will be the definition of a clear split for each function whether it is a) an operational function or b) a signalling function. All operator interfaces, regardless whether they are within a control centre or out in the field (e.g. mobile devices), shall be connected either to PE or to the systems level above PE (e.g. TMS).

Note: The possibility/need of an interface to APS that is realised e.g. in a Workbench operated within a control centre has to be analysed in a separate RCA operating concept.

PE is not only a direct interface for data exchange to and from APS. It also splits the required data exchange into data needed on operational level and data needed for discrete and safe handling in APS.

2.3.3 Delta

In contrast to the many existing direct interfaces between operational and signalling layer of today, PE standardises one single interface to and from APS and comprises a wide set of functions, covering an Infrastructure Manager's operational requirements, no matter whether this Infrastructure Manager deploys a TMS or not.

2.4 Operational harmonisation

2.4.1 Problem description

Today's historically evolved operational processes are a result of different operational needs, technical possibilities and options available to Infrastructure Managers. The approach of standardisation in this segment was in the past treated to standardise an interlocking platform such as EURO-Interlocking and INESS and the definition of a unified Standard Communication Interface for interfacing Control Centres (SCI-CC) within EULYNX.

Without a real operational standardisation, no uniformed interface between operation and securing of movements can be achieved. All derived products are built for and on specific operational rules and the so-called standardised interfaces between signalling layer and operational systems are more a summary of potential needed data bits with the lack of having a defined syntax and semantic. Thus, the engineering and safety approval effort still remains very high. In addition, several operator interfaces on the level of TMS but also on the level of interlocking exist. This complicates any operational usage by creating different operation principles with different human machine interfaces (HMI).

Standardisation of technical solutions and operations have been introduced with ETCS and the associated operational rules but still, Train Control must interface with the signalling systems. This cannot be a basis for a full standardisation between operation and signalling level.

In most cases, products are covering the specific operational needs, mainly driven from degraded situations and the national historical specialities. There is no platform or toolbox yet, representing a minimum set of unified operational and technical solutions.

2.4.2 Solution approach

Operational harmonisation among all stakeholders is a fundamental prerequisite to enable a generic safety logic, able to secure movements on any topology and thus, to significantly reduce configuration efforts. Technically, this means that there is no need for APS to manage hundreds of IM-specific rules to adhere to national processes. Therefore, the amount of engineering processes compliant to SIL 4 development can be reduced.

A coordination process between all Infrastructure Managers with the goal of operational harmonisation shall be established.

2.4.3 Delta

Standard operational processes not only promote interoperability with considerably less configuration and safety approval efforts but also enables a lean SIL 4 implementation and generic safety checks on the topology.

Additionally, this leads to that architecture delta towards a full operational standardisation of the core functions of RCA instead of only partial harmonised rules and many adaptions between products and operational rules by each Infrastructure Manager or project using existing products.

2.5 Safe localisation information

2.5.1 Problem description

Localisation of trains is currently performed by different technologies. In general, they are referenced as part of the signalling equipment and independent from the used standard solutions like trackside train detection systems with axle counters or track circuits. In addition, ETCS allows a finer resolution of localisation information.

Further technologies shall be made available too.

An issue is the safe handling of these information. Safety in case of trackside train detection is performed indirectly with design rules. Safety in case of ETCS is treated as fulfilled by applying the ETCS toolbox, but current applications show a mismatch in the understanding between safety-related requirements and performance needs. This leads to a safety argumentation of this localisation information in those systems using this information, such as an RBC for instance and contradicts with the approach of a modular safety architecture that proposes a clear split of responsibility between trackside and on-board.

While widening this current approach on future localisation technologies, the complexity will grow and with the existing approaches to reach a uniform standard solution will never be possible. One goal of APS in RCA is having a simple, unified and safe trackside signalling system only dealing with different localisation information in a safe way.

2.5.2 Solution approach

As a prerequisite, APS will demand safe localisation information. Safe means in that context, that the level of safety is transparent for APS e.g. by getting any information on specific confidence intervals for the data received, including the overall approach of ensuring safety by the localisation system.

This guarantees:

- APS does not need any additional safety consideration and/or to add safety margins that would contradict the optimal operational usage (best infrastructure capacity utilisation)
- APS does not rely on information received from interfaced systems, when a higher safety level was assumed by APS and the difference was not transmitted transparently to APS
- APS can recognise the absence of safe localisation information and make safety-related decisions for on-going operation

The detailed handling of these information is shown in the subsequent chapters 4.1 and 4.2.

2.5.3 Delta

Instead of being part of the signalling solution, a full localisation system covering different technologies towards APS and other stakeholders is needed. The transmitted information must indicate the level of safety performed e.g. by correct determination of confidence intervals or measurement errors.

Thus, localisation is not only reduced to being a sensor. Localisation must fulfil the needs of the system working with the information like APS.

2.6 Computing Environment and Network

2.6.1 Problem description

Legacy signalling applications are using their own computation and communication platforms. This leads to different variants of platforms and a complex combination of any other applications installed in an IM's rail systems environment.

APS as a software-based application needs a computing environment and a communication network interfacing with different further parts of RCA and external entities.

2.6.2 Solution approach

One solution approach is that a computing environment and a communication network must be designed and made available for APS considering the requirements of a safety relevant system like APS. Ideally, this environment would be provided independently from APS for all parts of RCA (considering the safety-relevance of other RCA subsystems). APS assumes fulfilling of specific requirements enabling high-availability, safe handling, and cybersecurity functions by the computation environment.

Another approach is that APS runs as a new software suite on already existing hardware platforms and uses existing communication network. This implementation strategy doesn't solve the issue of complexity of hardware platforms for rail systems, but it can be a viable option for some migration scenarios.

2.6.3 Delta

In contrast to legacy application, with RCA an overall computing environment and communication network can be made available.

2.7 Radio Communication System

2.7.1 Problem description

RCA is based on the approach of radio-based data exchange between trackside and on-board. This shall enable an optimised and safe operation including data exchange at any position and any time.

The current transmission system for radio communication, GSM-R, is based on the outdated technology of the second generation of mobile communication. GSM-R will be only available for a short period of time (end of life). In addition, the spectrum of GSM-R is limited to the 900 MHz band with some additional frequency parts in the Enhanced GSM region for Rail services. Combined with the approach of using circuit-switched data transmission, with GSM-R, resources for radio communication are very limited in the current introduced version. Any optimisation having enough channels leads to small radio cells with a permanent handover.

A future-proof, stable and performant system with enough capacity (channels and bandwidth) is needed for RCA and APS. In addition, the problems concerning interferences and frequency coordination hindering an efficient operation must be solved.

2.7.2 Solution approach

Within the scope of Railway Mobile Radio (RMR) the frequency band for railway applications available is already extended to 1900 – 1910 MHz by the implementing decision (EU) 2021/1730. The successor of GSM-R, called Future Railway Mobile Communication System (FRMCS), must be developed and implemented stepwise in the Rail system for enabling the full usage of the advantages of RCA including APS.

Thus, the availability of FRMCS for APS is a prerequisite for an APS roll-out. GSM-R can be used for any transition period, but due to the future usage of packet-switched operation only, this shall be limited as much as possible.

The responsibility for fulfilling is named by the European Union (EU). Countries not being member states of the EU have agreements and fall under the same regulation. Several organisations are responsible for the detailed development of FRMCS:

- European Union Agency for Railways (**ERA**): Design Authority for ETCS and Authority for implementing ETCS and the radio communication system in the field, ensuring of making available a legal standard in time.
- Union internationale des chemins de fer (**UIC**): Major development partner of the ERA for FRMCS.
- Conférence Européenne des Administrations des Postes et des Télécommunications (**CEPT**): Organisation of the European Union responsible for enabling the presence and reservation of the frequency band including national cross-border agreements.

The relevant **Objectives** (see document [2]) for APS linked to the prerequisite are:

- APS@Support connectionless communication also via FRMCS
- APS@Support FRMCS for communication between track side and onboard

2.7.3 Delta

By introducing FRMCS, the circuit-switched data transmission will be changed to a packet-oriented service for better usage of the limited capacities in the frequency band. In addition, a higher data rate will be ensured by changing the mobile communication standard to the 4th and 5th generation.

2.8 Radio-based, ETCS-Equipped Train Units

2.8.1 Problem description

Several Train Control systems are installed on-board and trackside. The implementation of the European Train Control System (ETCS) was led by the aim to reach safety and technical compatibility. Today, several implementations exist with several versions of ETCS, accompanied by national requirements that contradict the technical compatibility. Efficient migration is hindered also by the minimal-step development by different Infrastructure Managers: The solution of signalling problems is done by introducing ETCS with only partial consideration of its application conditions and by specific implementation approaches considering legacy signalling systems including their historical problems. This leads to a late roll-out and sometimes to incompatible versions of on-board ETCS due to additional required national add-ons.

In addition, simple implementations of ETCS using the Level 1 in the trackside installations do not enable the full usage of operational advantages and will not bring any positive capacity effects for rail operation.

Based on these circumstances, on some railway lines, of CCS Class B systems are currently installed in parallel to ETCS. As a result, the Railway Undertakings do not suffer any pressure, to quickly instal ETCS on their vehicle for being allowed to operate them on such railway lines. This leads to the problem, that the prerequisite for APS (based on ETCS L2/L3) is not fulfilled on-board yet in all cases.

2.8.2 Solution approach

Three fields must be considered for reaching this target:

- ETCS versions/baselines covering enhanced functions (see below) must be made available
- Trains must be equipped with ETCS enabling radio-based operation, at minimum ETCS Level 2 for instance with a defined minimal baseline to be required by TSI CCS
- Various functions that are possible on the vehicle side must be presented transparently for the trackside, e.g., by introducing a new system version that identifies an improved ETCS version and simplifies the system integration between vehicle and trackside (Baseline Compatibility and Route Compatibility Check)

for handling the **Objective** (see document [2]):

APS@Presuppose the existence of a radio-based Train Control System (ETCS) assuming a continuous communication connection to each train on-board unit

Enhanced functions are handled within the full set of game changers defined within the scope of European CCS. Development and introduction of a legal version of ETCS beyond the planned TSI 2022 must be ensured. The responsibility for enabling is within ERA including supporting organisations like UNISIG. Enhanced functions of ETCS are for example:

- Enabling of ‘cab anywhere’
- Consideration of ‘always on’ for communication session
- Usage of ‘safe train length’ and ‘integrity’ ensured by the onboard equipment of a train unit by introducing a safe on-board localisation with an integrated solution between localisation and train control platform

Based on this development, on-board products must be made available by the different suppliers in time including the architecture in the vehicle for easy migration like given in the initiative of the Open CCS On-board Reference Architecture (OCORA).

For the **equipment** of trains with ETCS, several conditions must be considered. No contradicting national requirements and systems are to be required to reduce integration efforts and to enable a smooth and efficient onboard migration. In addition, the migration of vehicles must be ensured in advance to the implementation of APS trackside. Technical and commercial incentives must be given for equipping all trains operation on lines foreseen for APS within at least ETCS L2 compliant equipment before getting in operation. Programs for fast and cost-efficient roll-out of train equipment are needed.

For both, the enhanced functions and the in-time equipment of trains, a stable version of ETCS is needed covering the demands of the future system defined in RCA context considering APS and Automatic Train Operation (ATO). This can only be ensured by shifting the focus of ETCS development from taking over functionalities from old systems to the operational and technical requirements of a new CCS approach.

2.8.3 Delta

Following the fulfilment of this prerequisite of enabling an ETCS equipment, a full on-board signalling can be used with no need of lineside signalling and the enhanced localisation technologies can be made available for optimised track occupancy.

2.9 Systemwide ID-Management

2.9.1 Problem description

Each trackside and on-board subsystem must be addressed unique, enabling the correct data transfer and the correct consideration on information based on a specific installation.

Addressing needs a management of Identifications (IDs). For ETCS this is already present for trackside installations like balises and for the on-board with a specific address per ETCS installation on-board. For further parts like interlocking, addressing schemes are specific per Infrastructure Manager, depending on the technical solution and uniqueness is only ensured in smaller areas of installation.

Only for parts of the trackside installation and on-board terms of the various international registers (Register of Infrastructure – RINF and European Register of Authorised Types of Vehicles - ERATV) are common. The set-up of these register for having a central data storage is at the beginning too.

The growing number of installations, large areas handling by one system and a cross-system data exchange leads to the need of clear identification of the source of data. This is valid for normal and degraded operation and as well the further data acquisition by each stakeholder interested in data covering different business purposes like e.g. evaluation of system quality, supervision by authorities and failure analysis.

There is currently no definition or overall management present, considering parts of the signalling system not being mentioned by TSI CCS.

2.9.2 Solution approach

A systemwide ID-Management must be established for the overall Rail system. This means an exchange between parts of this ‘system” – like the cross-system exchange in present installations.

Due to the connection between subsystems in RCA, the ‘systemwide’ approach must cover in minimum RCA. RCA is a big part of innovation in the rail system, enabling the usage of this ID-Management in the overall Rail system. Thus, it must fit to further domains of the railway system outside of the Command-Control and Signalling domain too.

This shall cover a unique and unambiguous addressing within the RCA including all interfaced systems. From the perspective of APS several parts must covered:

- Respecting already present parts like the ETCS-ID-Management including change proposals to the range of the ID or the handling, in case the present standards are not suitable for roll-out in big clusters (Addressing on-board, handling of fixed installations, usage of functions like Temporary Speed Restrictions)
- Definition of suitable range of the used IDs for the various applications
- Addressing of fixed installations interfaced to APS
- Addressing for internal function purposes like abstracted objects
- Handling of interfaces to neighbouring legacy systems
- Processes for management of IDs like initial request, handling of ranges, unique association of IDs towards a user
- Tool chain for handling of associated IDs
- Processes and Procedures for automated update of registers handling with IDs

As a summary the systemwide ID-Management must focus on RCA, enabling the handling of the on-board and serving as a base for the overall Rail system.

2.9.3 Delta

The difference compared to today’s application is a complete coverage of all system elements with unique identifiers (full CCS) and thus enabling installations and roll-out in larger areas compared to today interlocking of RBC related dimensions.

The ID management shall not be a restrictive factor in determining system size.

3 Overarching APS Concepts

This chapter covers the subset of objectives from Annex A: List of objectives that affect the non-functional APS requirements. The focus of these requirements is on the fulfilment of the overarching business needs to significantly reduce the migration effort and the life cycle costs of the railway infrastructure. The general concepts on which APS is based, the resulting requirements and the delta to today's interlockings are described in the following subchapters.

First of all, object abstraction as the vital concept of APS has to be elaborated in order to understand further concepts introduced in this document. The same principle which was already introduced in chapter 2.1 that allows the production of unified, reference topology data is used for the inner workings of APS.

To abstract object information towards the Safety Logic of APS, a **translation** of object information of the railway network topology, switchable Field Elements and occupancy claims must be made and vice versa. In order to process various abstract object information, some of the abstracted objects will need to be **aggregated** to represent the current **operating state** on which **generic safety checks** can be made by APS' Safety Logic. Generic means that there is no differentiation required between objects of the same functional group. These main tasks (translation, aggregation, safety checks) shall be considered as independent functions.

This functional separation within RCA according to [3] results in five layers:

- Plan Implementation Layer
- Safety Control Layer
- Object Aggregation Layer
- Device Abstraction Layer
- Device Control Layer

The following layers are in scope of APS:

"Device Abstraction Layer:

Components in the Device Abstraction Layer translate commands and current states of the abstract devices to those of specific devices and vice versa. Components in this layer

- In some cases, implement functionality and interfaces defined in the CCS TSI or EULYNX specifications for interfacing the Device Control Layer
- Operate in real-time
- Enable modular safety by decoupling the specific behaviour of individual devices from the abstract logic used on this layer

Note: In order to provide such an abstract representation of the railway network topology, the same abstraction approach of device and object aggregation is being performed by the system and processes which provide the logical railway network topology towards APS and to other RCA components (see chapter 2).

"Object Aggregation Layer":

Components in the Object Aggregation Layer translate abstract object commands to abstract device commands, and aggregate current states from abstract devices into abstract objects. Components in this layer

- Operate on abstract representations of real-world elements such as switchable Field Elements and Movable Objects
- Aggregate different information streams from the layer below for enabling components in Safety Control Layer having an aggregated view on the operating state
- Operate in real-time
- Implement rules only through parameter values in abstract objects, not through IM-specific functions

"Safety Control Layer":

Components in the Safety Control Layer ensure a safe future state of the railway network by validating requests and commands, allowing validated requests and commands to reach the Object Abstraction Layer, and reacting to unsafe states of the railway. Components in this layer:

- Execute combinations of logical functions on strictly abstract representations of real-world elements such as switchable Field Elements and train units
- Publish the aggregated operating state of the railway especially to the Plan Implementation Layer
- Implement rules only through parameter values in abstract objects, not through IM-specific functions
- Operate in real-time
- Enable modular safety by decoupling the specific behaviour of individual devices from the abstract logic used on this layer

The main output in this layer is the evaluation and the granting or denying of Movement Permissions requested by Plan Implementation Layer. A **Movement Permission** is an authorisation for a particular train unit to move in a defined direction, with a defined speed, along a defined path (a contiguous stretch of Track-Edge-Sections) on the railway network topology. Thus, a safe movement path for a train unit is provided including all conditions under which its movement can be performed safely. A Movement Permission always refers to exactly one train unit. Safety Logic (SL) will perform a set of safety checks based on the operating state to secure a dedicated and safe movement path for a train unit. A description of the basic concept and semantics of a Movement Permission and safety checks can be found from chapter 4.3.3 onwards.

In order to translate different information such as for instance current states of specific devices or a variety of position information from train units required by APS, their abstract object information, aggregation and logical representation must be defined. This allows the **standardisation** of all involved interfaces which will be elaborated on in chapter 3.2.

3.1 Functional Independency

3.1.1 Objectives and System Requirements

Objectives	System Requirements
APS@Apply a generic safety approach in encapsulating smallest possible safety relevant functions in building blocks that allow a separate safety approval	$Any functionality not declared safety-relevant shall be realised out of scope from APS $APS shall be considered in the safety management process of RCA and be compliant with the safety requirements identified during the risk analysis $Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block
APS@Encapsulate minimal viable functionalities in building blocks to enable an individual configuration of the building blocks and simple interfaces	
APS@Demonstrate safety within the building blocks including its interface without knowledge or need of assumptions on the function of further building blocks behind the interface	$The combined use of functional building blocks shall not require an additional safety assurance $All APS interfaces shall be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact, and testable way $The behaviour of the individual APS components should be formally specified when required by formal validation
APS@Ensure process and system independence (control safe usage of track section regardless of how the rail network topology is physically realised)	$APS shall consider the provided Map Data as fail safe $APS functions shall be failsafe executable using any Map Data provided if the data complies to the application conditions
APS@Separate railway network topology data from functional code	$APS shall ensure that the application code only works on abstract representation of the topology $All APS interfaces shall be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact, and testable way
APS@Support independent updateability of Hardware, Software and Engineering Data	$APS must ensure Engineering Data independent approval $APS must ensure Software-independent approval $APS must ensure Hardware-independent approval $Ensure clear layering for transport, marshalling and application model
APS@Separate trackside assets from interlocking software	$APS shall ensure that the application code only works on abstract representation of the topology

3.1.2 Problem description

Today, the interlocking performs safety checks on a specific railway topology that is only applicable to this specific site. The safety logic is based on preconfigured track routes including all its dependencies such as (light) signals, point positions, operational feasibility, etc. This leads to a high number of dependencies between operational processes, railway production (execution of train movements), track layout and route protection resulting in an increased impracticality of upgrading individual components/subsystems or integrating new functionalities without having to change neighbouring (sub-)systems as well.

Furthermore, today's applications distinguish between route protection and train protection, both in a technical and functional sense. This stems from the historical split of the development of the two systems - interlockings were developed much earlier than train protection systems. This leads to high implementation efforts and a

kind of "ping-pong" of safety conditions and delimitations when changing existing (national) train control systems or implementing ERTMS standards.

3.1.3 Solution approach

The approach to solve these problems and untangle the dependencies between systems is to achieve a modular architecture of APS on an operational, functional and technical level.

To achieve a modular system architecture and to enable an appropriate allocation to logical (and ultimately physical) components during product development, APS's functions have to be easily separable. Hence, generic, small functional blocks have to be identified and grouped considering following aspects:

- Safety relevance
- Complexity
- Dependencies to other functions

The goal is to have functions that are characterised by a

- Small amount of input data,
- Simple processing logic and
- Simple (wherever possible binary) output.

Based on this, it's possible to trim down the scope of APS to safety-relevant functions with simple interfaces between them. Thus, unnecessarily high requirements for implementing non-safety-relevant functional blocks can be avoided because they are delegated to subsystems that fulfil a lower SIL. The APS' range of functions shall be kept to an absolute minimum to enable maximum independency from changes induced by connected subsystems (life cycle, new/changed Field Elements/technologies). This approach leads to the conclusion that APS shall not deal with operational or processual functions (e.g. dead-lock prevention, conflict resolving, operational optimisation of infrastructural usage).

Note: There will be safety relevant functionalities within the scope of RCA that are not realised by APS but in other components such as Object Controller for instance.

3.1.4 Delta

In comparison to today's interlockings the identification of the smallest, possible functional blocks allows

- Appropriate allocation to technical components according to SIL
- Simple combination of functional blocks to form a safe system
- Implementation of more functionalities on COTS products
- Exclusion of business logic from the interlocking
- Faster safety assurance

3.2 Standardised Interfaces

3.2.1 Objectives and System Requirements

Objective	System Requirements
APS@Consider open interfaces to integrate as much formats as possible	$All APS interfaces shall be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact and testable way $The behaviour of the individual APS components should be formally specified when required by formal validation
APS@Develop and commission standard interfaces	$All APS specifications shall be freely available to anybody at no cost. $All partners shall sign an open-source agreement at the very beginning of the project $All contributions to APS specifications fall under the agreed open-source agreement $No participant may claim any rights to the APS specifications or further work results openly published under the agreed open-source licence $APS shall provide information on its interfaces in such a granularity and format that it is suitable for target systems to consume the information correctly and efficiently $Ensure clear layering for transport, marshalling and application model
APS@Ensure functionality even in case of incomplete information due to limited functionality of interfaced components	$APS shall be able to process information of varying quality on its interfaces $APS shall provide information on its interfaces in such a granularity and format that it is suitable for target systems to consume the information correctly and efficiently
APS@Ensure interface compatibility to legacy interlocking systems still equipped with lineside signalling	$APS shall support the safe movement of a train unit from an APS Area of Control to an adjacent legacy signalling system and vice versa $The speed of a train movement shall not be limited due to the transition between an APS Area of Control to an adjacent legacy signalling system itself but only due to any rail network speed restrictions
APS@Use of existing infrastructure without the need of changes/alignment due to the use of APS	$APS shall process localisation information from existing TTD systems $APS shall not rely on the existence of localisation information from existing TTD systems to identify track occupancies $APS shall consider all safety relevant railway network usage conditions prior to safely granting a movement for a train unit $APS shall provide interfaces that are compliant to the TSI CCS $APS shall provide interfaces that are compliant to EULYNX interface specifications $APS shall not require an adaptation of the infrastructure when put into operation
APS@The building blocks and their interfaces should have as little version dependency as possible	$Ensure clear layering for transport, marshalling and application model $All APS interfaces must provide multi version support

Objective	System Requirements
APS@Enable usage of mix of different ETCS OBU system versions on line (migration facilitation)	$APS shall provide interfaces that are compliant to the TSI CCS. $APS support different ETCS system versions within the same APS Area of Control $All APS interfaces must provide multi version support
APS@Support EULYNX standards for interfacing with field elements via Object Controller	$APS shall provide interfaces that are compliant to EULYNX interface specifications $APS shall be able to process information of varying quality on its interfaces
APS@Separate data aggregation from data provisioning	$APS shall support different localisation technologies that may deploy different reference systems with different data formats on their interfaces $APS shall process localisation information from a variety of localisation systems and technologies $APS shall use a unified and generic representation of identified track occupancies, independent of the localisation technologies used $APS shall ensure that the application code only works on abstract representation of the topology
APS@Introduce generic capabilitiy-based interfaces	$All APS interfaces should be specified in an unambiguous, exact and testable way $Ensure clear layering for transport, marshalling and application model
APS@Support the AoC segment size of the interfaced Plan Execution	$APS shall support the segmentation of MAP data from interfacing systems
APS@Allow the replacement of different trackside devices implementations that comply to the standardised (transactor) interfaces with other implementations without effort	$APS shall provide interfaces that are compliant to EULYNX interface specifications $APS building blocks shall work independently of the functionality of neighbouring blocks, therefore no assumptions about dedicated behaviour shall be made $APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations
APS@Ensure network wide adaptability towards changes of the trackside CCS SubSys	$APS shall provide interfaces that are compliant to EULYNX interface specifications. $APS shall be able to process information of varying quality on its interfaces $All APS interfaces must provide multi version support

3.2.2 Problem description

See chapter 3.1.2 for the problem description.

3.2.3 Solution approach

APS interacts with internal and external components/subsystems over distinct interfaces. For all interfaces, detailed interface concepts and specifications either exist or are planned. The following sections briefly describe the interfaces from and to APS.

There are different, external interfaces to be considered:

- New interfaces defined in the context of RCA

- Existing, new and updated interfaces defined in the context of EULYNX to the switchable Field Elements or neighbouring signalling systems
- Existing, new and updated interfaces defined in the context of UNISIG, e.g. as subsets for the ETCS standard or the localisation system

New interfaces within scope of RCA are treated to be developed as FFFIS. In contrast, existing interfaces in legacy trackside signalling systems are partly defined as FIS only. In case interfacing APS towards a legacy system, no specific change in the legacy system and APS shall be made to avoid any additional integration efforts. Interfacing must be non-reactive. This can be achieved by using an adapter for transferring the information between both systems including adaption of the functional behaviour.

In general, interfaces used in the RCA architecture (see [3] for details) can be divided into different categories, independently if they will be defined in RCA scope or already existing:

Interface type	**Abbreviation**	**Content**
Standard Communication Interface	SCI	Handling the sending and receiving of requests and commands between two components/subsystems
Standard Authentication/Authorisation Interface	SAI	handling the authentication and authorisation between two components/subsystems
Standard Maintenance Interface	SMI	configuration and management interfaces
Standard Diagnostic Interface	SDI	diagnostic and monitoring interface
Standard Workbench Interface	SWI	interface to the workbench for external handling of railway operation and usage in fall-back operation
Standard Handover Interfaces	SHI	interface to a different instance of the same component/subsystem or a component/subsystem with similar functionality (interlocking, RBC)

This table serves as an overview of different kinds of interfaces having a complete list of types.

Note 1: A full architectural view on handovers and interfaces to different APS applications and towards neighbouring signalling system does not exist in the architecture yet and will be established in the future. The general concept for handling transition areas is to be developed in the detailed concept, thus a basic requirement is defined in this chapter.

Note 2: In addition to the external interfaces, several interfaces have been identified in [3] between the Safety Control Layer, Object Aggregation Layer and Device Abstraction Layer ad interim. This approach follows strictly the abstraction principle introduced at the beginning of chapter 3 in order to build small technical products. The eventually needed technical interfaces within APS will be defined in a later stage when forming discrete products. As for now, only the coordination of external interfaces is needed, thus the development of the concept is not hindered by the exclusion of internal interfaces.

The scope of APS within RCA is to align the development of the needed Standard Communication Interfaces as well as further interfaces needed for diagnostics.

Therefore, several external interfaces for APS will be developed in the context of RCA. Not all are mentioned in this document here.

A major interface is the **Standard Communication Interface – Command** (SCI-CMD). Through this interface, Plan Execution transmits requests to fulfil the Operational Plan originating in the TMS.

As an example, the following table contains an overview of the proposed functionality of SCI-CMD:

Description item	**Description content**
Full name	Standard Communication Interface - Command
Definition	SCI-CMD is an interface for handling requests and/or commands towards a component/subsystem of the Advanced Protection System (APS) e.g. to allow safe movements by discrete requests. SCI-CMD is used as external as well as internal interface from the point of APS.
Downstream (e.g. PE >> APS)	Request/Command state of Drive Protection Section Group e.g. for the abstracted Field Element to be drivable Request/Command of a Movement Permission for a Movable Object Request/Command of Usage Restriction Area Request/Command of Warning Area e.g. for a Train Driver or Trackside Person
Upstream (e.g. APS >> PE)	Provide operating state (entities: Drive Protection Section Group, Movement Permission, Movable Object, Usage Restriction Area, Warning Area) Information on rejected requests if these have violated any rules at a certain time

Furthermore, compliance to EULYNX interfaces has to be considered. EULYNX-compliant interfaces are used for two purposes:

- Enabling the reuse of existing interfaces to Field Elements including existing Object Controllers, e.g. SCI-P for interfacing points and SCI-LC for interfacing level crossing protection facilities
- Interfacing existing signalling equipment in neighbouring Area of Control for migration purpose, e.g. SCI-ILS for interfacing a legacy interlocking

Besides EULYNX standards, also the TSI CCS including future amendments must be considered due to APS' ability to interact with the on-board CCS system (ETCS as Train Control System). Mainly the following interfaces are to be considered:

- Interface between trackside and on-board ETCS, e.g. defined by UNISIG Subset-026 for exchange of ETCS data, the associated documents for radio-based communication and the in future established standard for localisation system interface
- Interface to neighbouring signalling equipment for radio-based Train Control (here a Radio Block Centre) e.g. by respecting the UNISIG Subsets-039 and -098 including the needed configuration matrix to be applied

The creation of UNISIG-compliant interface specifications serves as the foundation to enable APS to operate with vehicles equipped with ETCS.

3.2.4 Delta

The improvement in the information flow based on the introduced external and internal interfaces can be demonstrated best with some examples on how the mapping of interfaces and the information flow to the architecture introduced in [3]:

- **SCI-CMD** of RCA
    - Information flow between the Plan Execution and the Safety Logic of APS is considered here
    - Ability to handle a request for a specific Movement Permission in order to enable APS to authorise a train run from Plan Execution (downstream)

    - Ability to provide the APS Operating State, i.e., the acceptance/rejection of Movement Permission Requests, the setting state of Field Elements, etc. to Plan Execution (upstream)
    - The SCI-CMD enables the clear split between operational responsibility outside of APS and the safety responsibility in APS
    - The SCI-CMD enables best possible operational view of the operational systems by transmitting any information present in APS
- **SUBSET-026** of UNISIG
    - Information flow between APS and the ETCS on-board equipment of a train unit is considered here
    - Transmitting a radio-based Movement Authority by APS to the train unit (downstream)
    - Receiving an ETCS-Position Report sent by the train unit as a base for object aggregation (upstream)
    - The usage of UNISIG SUBSET-026 is limited to the needed functionality of the subset of functions of the ETCS toolbox
    - UNISIG SUBSET-026 will also consider the game changers introduced in the ETCS toolbox being relevant for APS and overall RCA
- **SCI-P** defined in EULYNX
    - Interfacing APS and an Object Controller interfacing a point machine
    - APS has the ability to send a request for a specific point position, regardless of how many point machines are installed (downstream)
    - The interface enables APS to receive certain states of a specific Field Element interfaced via an Object Controller
    - The usage of SCI-P in example is limited to the control of switchable Field Element only without any respect of additional system behaviour introduced in the technical systems based on the EULYNX toolbox. Thus, it is used as a simple interface for control of switchable Field Elements only.

3.3 Generic Product Assurance

3.3.1 Objectives and System Requirements

Objective	System Requirements
APS@Enable a safe system and its safety assurance based on building blocks in order to minimise effort for safety assurance	$Ensure safety relevance of each component to prevent components from suddenly becoming safety relevant in a later implementation $Any functionality not declared safety-relevant shall be realised out of scope from APS. $The combined use of functional building blocks shall not require an additional safety assurance
APS@Allow the replacement of components without changing the system safety case	$The combined use of functional building blocks shall not require an additional safety assurance $All APS interfaces should be specified in an unambiguous, exact and testable way
APS@Ensure safeguarding of movements for any railway network topology that is compliant to the safety-related application conditions	$APS functions must be failsafe executable using any Map Data provided if the data complies to the application conditions $APS shall consider all safety relevant railway network usage conditions prior to safely granting a movement for a train unit
APS@Minimise effort for safety assessment	$APS must ensure Engineering Data independent approval $APS must ensure Software-independent approval $APS must ensure Hardware-independent approval $Safety checks shall be independent of operational procedures $The integration of building blocks with their own safety assurance shall result in a safe system that does not require further safety approvals. $The combined use of functional building blocks shall not require an additional safety assurance
APS@Perform generic hazard management by an overall system authority	$APS shall be compliant with the safety requirements identified during the risk analysis
APS@Consider hazards of current solutions and reduce impact through system design	$The safety processes of the APS solution design (supplier activities) and the APS concept design (IM activities) shall be aligned $APS shall be compliant with the safety requirements identified during the risk analysis. $APS shall be developed using a robust software development process according to CENELEC standards
APS@Delegate non-safety relevant functions to planning system	$Safety checks shall be independent of operational procedures
APS@Reduce need of Infrastructure Manager related hazard evaluation	$APS risks shall be limited to safety-relevant aspects without considering business-critical risks to the railway performance
APS@Support exchange of hardware and software components with the same functionality with less need of system approval	$The combined use of functional building blocks shall not require an additional safety assurance $All APS interfaces should be specified in an unambiguous, exact and testable way

Objective	System Requirements
APS@Consider hazards of current solutions and reduce impact through system design	$The safety processes of the APS solution design (supplier activities) and the APS concept design (IM activities) shall be aligned $APS shall be considered in the safety management process of RCA and be compliant with the safety requirements identified during the risk analysis

3.3.2 Problem description

The safety assurance process of systems and products requires the proof of compliance to relevant legislation, standards, guidelines, best current practice, and customer's specifications. This proof is referred to as safety case which can be differentiated according to various stages of system or product development and application:

- Product design and development: The generic product safety case provides evidence that product design and validation meet its safety requirements. It covers the application-independent aspects (defined generic rules) of the product as well as its interfaces if it is designed to interface and operate with other products.
- Generic Application Design: The generic application safety case provides evidence that a system or product application's design and validation demonstrates its safe operation in a class of application with defined application rules. For instance, the generic application case of system 1 (consisting of product A and product B) uses the product safety cases of A and B to demonstrate application-independent evidence.
- Specific application design and implementation: The specific application safety case provides evidence that a (sub-)system's design and implementation meet the safety requirements for a specific application on a particular railway line. It also covers manufacture, installation and testing of the application as well as the necessary operating and maintenance processes/facilities.

From this "multilevel" approach, it can be concluded that the effort for safety assurance rises if there is a high number of requirements specific for an application on several railway lines. Due to this, the current assurance processes in the railway sector are getting considerably more complicated, expensive and onerous.

3.3.3 Solution approach

From the preceding elaboration of the safety assurance process, it can be concluded that in order to reduce the assurance effort sustainably, it is paramount to reduce the number of Infrastructure Manager specific requirements for a system. This can be achieved by a number of design decisions for APS:

- Generic safety logic without considering national adaptations and excluding operational rules (e.g. dead-lock prevention, conflict resolving, operational optimisation of infrastructural usage)
- Definition of small building blocks, each fulfilling one function
- Abstraction of device-specific behaviour

The concepts on which the safety logic is based on, have been introduced in the previous chapters (abstraction, operating state, etc.) and can be referenced for understanding the processing logic of APS:

For each request, the Safety Logic compares basically two geometric extents: the one requested with the one represented in operating state. This geometric overlap is being checked against defined rules and if these are being violated or not. In case that there is no violation identified, APS grants the request. The "defined rules" are called Safety Rules and the "comparison" is called Safety Check hereafter.

The Safety Rules are based on some principles, like for instance that the Movement Permissions from different train units do not overlap from the geometric extent except in some degraded situations.

Examples for a safety related rule:

- A switchable field element must be in the correct position prior to a Movement Permission request. Hence, the requesting system must request that correct state/position prior to requesting a Movement Permission.
- Possible flank protection measures required in order to safely pass e.g. a switchable field element must be set and requested before requesting a Movement Permission.

Using generic Safety Rules also eliminates the need for a distinction between distinguished shunting movements and train movements (see chapter 4.3), which means that a lot of today's interlocking functionality can be shifted to the processing logic of TMS, including PE.

3.3.4 Delta

In comparison to today’s interlockings the effort for safety assurance for any future RCA applications shall be reduced under consideration of the following approaches:

- Reduction of the number and complexity of checking rules to a minimum – only basic (generic) rules
- Prolonging the possible life cycle and implementation of business logic on the side of the requesting systems (TMS, PE)
- No business logic in APS: The requesting system must make sure that safety related rules are not being violated to prevent a reject from APS.

3.4 Independency from Project Planning

3.4.1 Objectives and System Requirements

Objective	System Requirements
APS@Separate the safety logic system from operational planning systems	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block. $The combined use of functional building blocks shall not require an additional safety assurance $Safety checks shall be independent of operational procedures
APS@Use the same high parameterisable safety level for any railway network topology (includes safe control at any time of existing and interfaced trackside assets)	$The definition and configuration of safety conditions to be checked by APS shall not contain site or location specific references
APS@Provide a uniform user operating concept, independent of the site-specific rail network	$APS shall provide identical functionalities for any kind of operational movements $Safety checks shall be independent of operational procedures
APS@Enable implementation of APS on existing track layout without changing it	$APS shall provide a default configuration that allows safe movements on any railway network topology that complies with the defined application conditions $APS shall support the safe movement of train units on an arbitrary railway network without major adaptations of existing trackside assets

3.4.2 Problem description

Today's railway project costs are driven by high expenses on project planning, design and creating engineering data due to the diverse product landscape in the sector. Existing product capabilities have to be extended on a regular basis to satisfy site-specific requirements which often, almost certainly, leads to the need of changes for neighbouring products or systems. IMs, integrators, and manufacturers have to manage increasingly complex systems which render the following tasks much more difficult:

- IM: Necessary changes to systems and their effects on interfacing systems and rollout alignments have to be anticipated and planned well in advance.
- Integrator: Release changes of particular products and their effect on interfacing systems have to be managed.
- Manufacturer: New features have to be implemented into a product considering its overall product strategy and without affecting the already implemented functionalities.

3.4.3 Solution approach

Firstly, the shift of effort towards Map data provision introduced in chapter 2 already results in a massive reduction of project planning effort compared to today: All RCA subsystems use a common topology database, the Map Data, so that the overall effort for implementation, testing, troubleshooting, maintenance, etc. can be reduced.

Secondly, by removing fixed signals and track vacancy detection devices, a further reduction of the project planning effort can be achieved.

Thirdly, with the elimination of preconfigured track routes including all its dependencies to trackside assets (light signals, point positions etc.) there is no need to define control tables and implement route paths into the interlocking. Safety rules and safety checks shall be defined generically, so that they are applicable regardless of the railway network topology or site-specific characteristics. There will be a set of configurable safety rules

in order to allow adaptation to specific IM's needs. Configurable in the context of safety checks and safety rules refers to the following adjustments:

- Safety rule applicable or not
- Safety rule applicable when condition X is fulfilled
- Safety rule not applicable when condition Y is fulfilled

Example of a configurable safety rule:

Different IMs may have different requirements for flank protection when granting a Movement Permission; IM A has no requirement for any sort of flank protection, IM B requires flank protection for speeds above 80 km/h and IM C for speeds above 120 km/h.

3.4.4 Delta

In comparison to today's interlockings the effort for site specific configuration for any future RCA applications shall be minimised under consideration of the following improvements:

- Reduced effort to generate Map data
  - No multiple sources of Map data, see chapter 2.1
- Reduced effort to generate the interlocking safety logic
  - No need to implement control tables (preconfigured route paths) into the interlocking's processing logic
  - Allowing the shift to implement specific rules for operation to a non-safety-relevant system which requires less exhaustive engineering processes
- The geometric extent of a Movement Permission can be freely defined by the requesting system.
  - More operational "flexibility" to optimise the use of the railway network in long- and short-term planning
- No geographical and site-specific configuration data and project planning for safety related checks

Note: The term "no site-specific project planning" doesn't mean that there are (and probably always will be) no site-specific conditions to be respected in some cases.. It rather means that there will be one or multiple safety rules dealing with this topic, but they will be applicable to any site and station.

3.5 Life Cycle Cost

3.5.1 Objectives and System Requirements

Objective	System Requirements
APS@Allow the replacement of multiple legacy interlocking with one single APS	$Within the Area of Control, APS shall support minimally 1250 switchable field elements $Within the Area of Control, APS shall support minimally 3.000 TTD $Within the Area of Control, APS shall support the safe production of minimum of 75 simultaneous train units (moving, stopped) per hour $APS shall be interfaceable to a various number of present Object Controller in compliance to the EULYNX standards, interfaced to different legacy interlocking systems
APS@Enable cab-signalling for all movements	$APS shall provide interfaces that are compliant to the TSI CCS $APS support different ETCS system versions within the same APS Area of Control
APS@Enable changes, adaptations and extensions throughout the life cycle of the building blocks	$Ensure an agreed and committed life cycle policy between all suppliers for investment protection $All APS interfaces must provide multi version support $Future sematic changes shall under no circumstance require changes in the interfaces $APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)
APS@Enabling predictive maintenance by data capture for increasement of overall availability	$APS shall provide quantities and frequencies of processed data towards Monitoring $Provisioning of measurement data must not influence the performance of APS
APS@Overlapping technology lifecycle profiles must be respected by the system design	$All APS interfaces must provide multi version support
APS@Support the TSI CCS enhancement “cab anywhere” (e.g. UNISIG-CR 1367)	$APS shall provide interfaces that are compliant to the TSI CCS $APS support different ETCS system versions within the same APS Area of Control
APS@Use standard interface towards Field Elements to separate the lifecycles of hardware and software components	$APS shall provide interfaces that are compliant to EULYNX interface specifications.
APS@Capturing of operational data covering RAMSS performance requirements and assumptions during operation	$APS shall provide quantities and frequencies of processed data towards Monitoring $Provisioning of measurement data shall not influence the performance of APS
APS@Usage of different train localisation technologies for reduction of costs for trackside train detection system	$APS shall not rely on the existence of localisation information from existing TTD systems to identify track occupancies $APS shall provide interfaces that are compliant to the TSI CCS $APS support different ETCS system versions within the same APS Area of Control

Note on requirements for objective APS@Allow the replacement of multiple legacy interlocking with one single APS: The RAMS values are a rough estimate based on operational data of the Swiss Federal Railway (SBB) from 2019 assuming that

- *Field Elements (13.000), TTDs (90.000) and train units (101.000 trains/day) are distributed equally across the interlockings (510)*
- *One APS replaces 50 legacy interlockings*

3.5.2 Problem description

The life cycles between different railway (sub-)systems are not synchronised between each other due to the historically staggered evolvement of the railway system, and thus the gradual integration of new functionalities and components, too (see chapter 3.1.2). As a result, there is a high dependency between life cycles which leads to significant costs for asset managers. For instance, an IM cannot replace an end-of-life interlocking without adapting the interconnected RBC, resulting in additional development and integration costs. Due to the high interdependencies, today's railway infrastructure is incredibly complex and expensive to manage.

3.5.3 Solution approach

The first solution concept is to enforce a strict separation of concerns between business logic and safety logic, which results in separate life cycles for both. Thus, enabling fast, innovative and cost-effective improvements of the business logic and reduced development and maintenance costs for APS.

The need for operation in degraded situations due to unavailability of parts of the systems, e.g. due to risks caused by age and wear of components/subsystems used, can limit safety. Thus, all parts must be considered with certain limited non-availabilities and monitored if deemed necessary. This leads to a strong dependency on timely and swift maintenance activities for enabling safe and reliable operation. All failure modes must be known and checked for any unwanted influence on the overall safety of the system.

In a first step, the required "Mean Time Between Failures" (MTBF) and "Mean Time To Repair (MTTR) for APS will be derived for the overall APS application and later detailed per technical product. These requirements must be demonstrated and respected by detailing allowed operational degraded situations, including their definition of any limitations, like maximum time or sequence of operation in fallback scenarios.

During operation, e.g. in fallback scenarios, there is an operational interface between Infrastructure Manager and Railway Undertaking present, the calculated availability/reliability values must be documented. Thus, the supervision of the introduced capability of the CCS equipment (trackside and onboard) including RAMS performance monitoring is enabled.

Maintainability and the linked needs for maintenance facilitate the overall safety of the system. Each product must be maintainable with appropriate maintenance activities that are in line with the needs of Safety, Reliability and Availability as well as the operational scope and usage of the system. This is a major task in product design.

Nevertheless, the main issue in early detailing of APS is enabling of data capture for having a fundamental base for any decision making on maintenance activities in the field. This means, that APS must be able to provide information on the behaviour of its system in order to assist the planning of maintenance activities including the reduction of down-times.

As the responsibility of managing and handling maintenance lies with the Infrastructure Managers, an early coordination of already available empirical maintenance data, like ETCS Level 2 equipment that is already deployed, is highly recommended. In addition, since the radio channel is part of the overall function (see chapter 2.7), also, empirical data of the Railway Mobile Radio (RMR – including GSM-R and FRMCS) is needed in order to reduce impact on operation based on unavailability, radio coverage issues and the associated maintaining of the radio system. This reduces impact on operation and costs for maintenance activities

3.5.4 Delta

With the separation of business logic and safety logic and appropriate RAM planning, a high grade of independency of changes from interconnected subsystems (life cycle, new/changed Field Elements/technologies) can be achieved. As a result, the costs for IMs for installing, adapting and maintaining the infrastructure will decrease compared to today.

3.6 Automation

3.6.1 Objectives and System Requirements

Objective	System Requirements
APS@Handle failures and degraded modes of other RCA SubSys efficiently	$APS shall disclose and support the handling of failures from interfaced RCA SubSys
APS@Handle internal failures and degraded modes efficiently	$APS shall disclose and support the handling of internal failures
APS@Minimize the transfer of one or many safety responsibilities to a human operator even in degraded situations	$APS shall support and provide guidance for manual operation on a fallback user interface $APS shall support the transfer of Safety Responsibility in an automatic way
APS@Support interfacing to additional field elements during runtime	$APS shall consume MAP data updates during runtime
APS@Support published changes in Map Data (new, change, delete) during runtime without impact on operation	$APS shall consume MAP data updates during runtime
APS@Update of safety demonstration documentation after replacement automatically	$APS documentation shall be generated automatically and stored in an efficient document management system
APS@Use interfaces with automatic adaptions and internal intelligence for interfacing different versions of building blocks without the need of upgrade existing building blocks based on change in interface	$All APS interfaces must provide multi version support $APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)
APS@Disclose incompatibilities between building blocks and SubSys and their interfaces (i.e. incompatible software versions, incompatible protocol versions)	$APS shall support the automatic identification and recognition of different system configurations and versions during runtime $APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime
APS@Ensure the generation of a fail-safe operating state after a reboot	$APS shall recover efficiently after a reboot $APS shall continuously provide and monitor the current operating state including during the initialisation phase, re-boot and after changing interfacing (sub-)systems

3.6.2 Problem description

Today there are many manual tasks necessary throughout the life cycle phases of products and systems used in the railway. They create additional costs for the IMs as well as for manufacturers and integrators. Predominantly, the following areas are concerned:

- Generating overhead costs during degraded situations: The responsibility shifts to a human operator, resulting in a huge amount of paperwork, specific operational procedures that must be memorised by the staff and reduced railway performance and safety

- Interruption of railway operation due to integration tests and the need to change engineering data
- Prolonged duration and frequency of commissioning due to inefficient initiation and inauguration processes after release changes, system start-ups, rebooting after system crashes, etc.
- Additional effort in updating of product documentation, requirement tracing, test cases, safety documentations, etc. after making changes to the system or individual products

3.6.3 Solution approach

In order to tackle the previously mentioned areas of concern, it is intended that APS supports the usage of various technologies and architectures with the aim to minimise the transfer of one or many safety responsibilities to a human operator even in degraded situations.

Note: Though APS still offers the possibility to allow the transfer of one or many safety responsibilities to a human operator or to a third-party system, it should be able to cope with as many degraded situations as possible.

Also, the recovery from degraded modes should be handled efficiently by APS through an optimised inauguration process.

Furthermore, APS should enable automatic compatibility checks of configurations/versions of interacting systems and products to simplify and speed up the commissioning. Especially because APS depends on fail-safe topology data (see chapter 2.1), the updating of topology data has to be possible at runtime.

Lastly, there should be an appropriate document management system established which supports generating product and system documentation automatically.

Note: The resulting, non-functional requirement for the APS documentation will be exported to the appropriate cluster, presumably to methods and tooling (M&T cluster)

3.6.4 Delta

By implementing a higher degree of automation in different stages in the product life cycle (development, integration, operation) it is possible to handle recurring tasks like system updates, operation in degraded modes and system documentation more efficiently than today.

4 Solution concept APS

In this chapter a set of requirements for APS are derived from the business objectives listed in Annex A: List of objectives. This chapter covers the problems of today's situation, the proposed improvements to solve the aforementioned problems and the resulting requirements (tagged with "$Requirement-Keywords") for each category of objectives, and thus for each objective.

Core Principle 2 – Represent Current operating state

APS must be able to import Map Data of its specific Area of Control (AoC) from a central data source and represent this data in the so-called operating state. Operating state is a fail-safe logical representation of the physical railway network and all its capabilities, limitations, states and occupancy claims within the AoC:

- Capabilities: Are derived from the topological data (source: Digital Map) --> see chapter 2.1
- Limitations: Reduced capabilities derived during runtime from various sources (sources: NOT Digital Map, but human operators for instance) --> see chapter 4.2
- States: Current states and state changes derived from switchable field elements --> see chapter 4.3.3
- Occupancy Claims: current occupancy claims due to for instance physical occupancy of a train unit, maintenance work areas, track closures) --> see chapters 4.1 and 4.2

The following subchapters describe the main objectives and solution approaches to achieve a current operating state in APS.

4.1 Occupancy claims identifiable with localisation technologies

There are various causes of occupancy claims of a railway network within an Area of Control of an APS that can be identified using localisation technologies:

- Physical objects such as train units, identifiable with Trackside Train Detection (TTD) and/or onboard localisation functionality
- Physical objects such as track workers, machinery that are not identifiable with TTD but with future localisation technologies Or for which a geometric extent of the railway network has been protected to prevent any collision

4.1.1 Objectives and System Requirements

Objectives	System Requirements	Subchapter
APS@Consider continuous onboard localisation information (speed/extent)	$APS shall process on-board localisation information for aggregation of the track occupancy $APS shall support continuous localisation information to represent track occupancy	Track Occupancy
APS@Enable usage of train integrity information for optimised track occupancy without the restriction of fixed signalling blocks	$APS shall use train integrity information provided by on-board or trackside for aggregation of the track occupancy $APS shall enable track occupancy independently from fixed signalling blocks definition $APS shall release each section of a secured route path after safely identifying its clearance based on calculated safe rear end	Track Occupancy

APS@Ensure integration of new localisation technologies that will only emerge in future years	$APS shall use on-board localisation information for aggregation of the track occupancy $APS shall be able for interfacing new localisation technologies $APS shall represent any track occupancy as generic representation to be as independent as possible from formats of localisation devices	Track Occupancy
APS@Guarantee railway operation with a mixed ETCS level approach (L2/L3) of trains and rail network	$APS shall operate on different lines equipped with different ETCS level starting from Level 2 $APS support different ETCS system versions within the same APS Area of Control $APS shall support different ETCS levels simultaneously	Track Occupancy Safety Checks - Communication
APS@Provide Ability for safe train movement on arbitrary railway network topologies with at least one clear-track signalling or localisation technology installed	$APS shall be able to identify track occupancy with at least one trackside train detection system or localisation technology installed in the Area of Control $To represent track occupancy, APS shall be able to use a mix of trackside train detection system and localisation technologies installed in the Area of Control $APS shall support the aggregation of track occupancies along tracks not continuously equipped with trackside train detection system in conjunction with other localisation technologies	Track Occupancy, Object Aggregation
APS@Reduction of CCS trackside equipment on a needed level for operation by gaining capacity not only with standard CCS trackside enhancements (e.g. trackside train detection sections, shorter routes)	$APS shall use on-board localisation information for aggregation of the track occupancy $APS shall enable operation without the need of installed contiguous trackside train detection system $APS shall enable operation without the need of lineside signalling system $APS shall not limit the start and end of movements to specific positions in the Area of Control	Track Occupancy Safety Checks – Route Setting & Protection
APS@Support different localisation systems and localisation technologies for trackbound and non-trackbound objects in order to represent safely non-occupied track segments	$APS shall use on-board localisation information for aggregation of the track occupancy $APS shall be able for interfacing new localisation technologies $APS shall process mobile localisation device information of trackbound objects for aggregation of the track occupancy $APS shall process mobile localisation device information of non-trackbound objects for aggregation of track occupancy	Track Occupancy
APS@Support future train integrity and safe length information from the very beginning	$APS shall be able to represent track occupancy using safe train length information $APS shall release each section of a secured route path after safely identifying its clearance based on train integrity information	Track Occupancy
APS@Support only of ETCS Level 2 and 3 (also mixed on the same line)	$APS shall operate on different lines equipped with different ETCS level starting from Level 2 $APS shall support different ETCS levels simultaneously $APS shall only support ETCS levels equal to or higher than L2	Safety Checks - Communication

APS@Support the aggregation of multiple localisation information in order to represent the entire occupancy claim of train units	$APS shall support the aggregation of track occupancies along tracks not continuously equipped with trackside train detection system in conjunction with other localisation technologies $APS must represent any track occupancy in a fail-safe way	Track Occupancy
APS@Support the securing of route paths with any geometric extension with no need having a fixed start and end point defined by lineside signals	$APS shall enable operation without the need of lineside signalling system $APS shall not limit the start and end of movements to specific positions in the Area of Control $APS shall release a section of a secured route path after safely identifying its clearance based on train integrity information	Safety Checks – Route Setting & Protection
APS@Clear secured route path immediately when clearance has been identified (i.e. using safe train length, localisation tag) in order to maximise track capacity	$APS shall release each section of a secured route path after safely identifying its clearance based on train integrity information	Safety Checks – Route Setting & Protection
APS@Enable usage of train length and integrity information for optimised track occupancy without the restriction of fixed signalling blocks and/or train detection sections	$APS shall consider safe train length information and integrity state for object aggregation for efficient track occupancy	Track Occupancy

Note: Concerning the mentioned "localisation tag" within the objective, this is assumed as a specific device within the localisation system and for APS the specific used technology does not appear for the function.

4.1.2 Problem description

Today, occupancy claims of the railway network can be derived from various trackside and/or train-based sources that show the following determining conditions.

- Trackside Train Detection equipment:
  - Occupancy detection only for fixed geometric extensions possible
  - Exact location of train unit within fixed geometric extensions unknown
  - No train unit information available
  - Reliability strongly influenced by environmental conditions such as leaves, snow, sand or dirt (particularly with track circuits)
- Current vehicle-based localisation equipment (ETCS Train Position Reports)
  - Termination of communication channel between train and trackside, e.g. after end of mission/mode change
  - Missing/Invalid position information after e.g. start of mission
  - Manual entries of train data
  - Train integrity information

APS will need to determine and differentiate safely occupied from non-occupied track segments to safely grant Movement Permissions, using existing localisation technologies in order to allow a migration towards a system environment according to the Reference CCS Architecture (RCA). In addition to conventional trackside train detections systems, this concept foresees the integration of further safety hazard detection systems already existing and/or planned to be installed such as avalanche detection systems, rockslide detectors and so on. Integration shall be possible in the way that such existing systems are interfaced with the aid of Object Controllers.

Note: It is yet to be defined, whether in case of an identified avalanche for instance, each track section surveyed by this/these system/s could e.g., send a Usage Restriction Area Request via Transactor towards Object Aggregation directly to APS or whether it would send an information to PE which would then either send a Usage Restriction Area Request to APS or develop another solution approach.

4.1.3 Solution approach

4.1.3.1 Proposed representation of a track occupancy

An occupancy claim is a track section or uninterrupted sequence of track sections with a geometric extent greater than zero. Occupancy claims shall be represented in an abstract manner in order to have as few dependencies as possible from localisation technologies. An occupancy claim can be represented either as a spot location or as a geometric extent on the Map Data in the operating state, depending on the localisation information provided. Occupancy claims arise from

- Track-bound objects on a track section
- Non-track-bound objects on a track section

Track-bound objects in the APS context are localisable train units and road-rail vehicles when on the track (not localised track-bound objects cannot be placed on the track). Non-track-bound objects in the APS context are localisable humans, road vehicles, road-rail vehicles off the track and construction equipment.

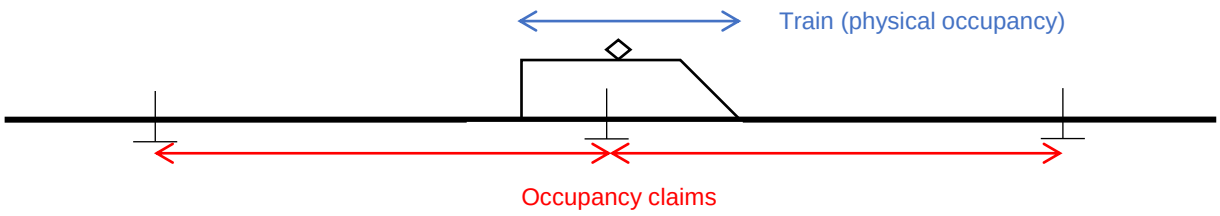

Figure 2: Generic representation of an occupancy claim

Additionally, occupancy claims can arise from

- Non-track-bound objects within the clearance gauge of a track section

However, the use cases when it makes sense from the operative and safety perspective to represent such objects as an occupancy claim are to be investigated at a later stage.

4.1.3.2 Proposed general working principle

Subsystems in the device abstraction layer will abstract technology-dependent localisation information (e.g. ETCS Train Position Reports, Trackside Train Detection sections, Geo-Coordinates) into one position on an Edge or into a geometric extent on 1..n Edges. The component Object Aggregation (OA) receives therefore potentially multiple localisation information about the same train unit and shall fulfil two main requirements:

- Represent instantly any received occupancy claim in the operating state.
- Aggregate occupancy claims into one logical representation of a train units occupancy claim if safely possible. This will allow to issue granted Movement Permissions to the corresponding train unit. In the further course of this document, this logical representation is generally called **Movable Object** (MOB).

Depending on the available localisation information content, Object Aggregation will be able to capture a unique identifier of the physical train unit which causes that occupancy claim (e.g. the ID of an onboard unit, further future identifier). Hence the life cycle of a MOB will depend on the availability of localisation information over time.

Example: When consuming track occupancy information from TTD equipment plus Train Position Report (TPR) of a starting train unit (assuming the train unit is not always reporting), assuming there is still the need to perform a ‘start of mission’, it may not be clear that the two received occupancy claims belong to the same train unit; hence Object Aggregation would generate in the operating state two different MOB’s that geometrically overlap.

To safely check if a route path is free of any occupancy or not, it is of no importance if an occupancy claim is represented as one or multiple MOB but that the occupancy claim **is** represented in the operating state. Only

when granting and communicating a requested Movement Permission, APS must ensure that the intended train unit receives its dedicated Movement Permission.

In the above example, the aggregation of multiple localisation information (sources: TTD, TPR) into a single MOB becomes possible after the physical train unit starts moving along its path.

MOB will be updated immediately by Object Aggregation after every update received (e.g. position update, speed update).

Note: The MOB position in operating state will be used by APS to automatically shorten cleared MP extents (see also chapters 3.6 and 4.3.3.3)

4.1.4 Migration

APS will be able to process various localisation information from multiple different localisation technologies from the very beginning and will be able to aggregate them in order to e.g. represent an entire train unit. Hence an IM using APS could adapt new localisation technologies or remove existing ones without the need to change the existing APS implementation but eventually to add an additional transactor for this specific localisation technology.

The functionality 'Object Abstraction' enables APS to safely represent any occupancy claim in the operating state, independent of the existing localisation technologies. The core functionality 'Object Aggregation' processes one or multiple occupancy claims with geometric overlap regardless of its origin to represent a Movable Object in the operating state.

Important to note is that Object Aggregation will be able to represent safely partially occupied TTD sections when processing today's available ETCS Train Position Reports from a train units front end. When safe train lengths and integrity information become available, Object Aggregation will be able to do the same for the train unit's rear position. After deploying APS, the move away from TTD installations can be done without the need of any configuration adaptation or additional approvals.

Note: It is open at this point in time, how localisation information from individual, coupled vehicles, (e.g. digital coupling, mobile localisation devices fit to train units or single vehicles), will be sent to trackside; (e.g. as one information containing front-, end-position, lengths or all information individually)? However, this will not affect the proposed architecture but the required functionality for Object Aggregation as part of APS.

Adaptation will be required in the (standardisation of) graphical user interfaces, where today in the majority of signalling systems only states of TTD systems are being represented. With APS and additional localisation technologies, there will be potentially more occupancy information available and to be represented in the human machine interface.

4.1.5 Degraded modes

Localisation information will be sent to and received by APS in different timely manners; occupancy claim states of TTD systems will be constantly valid, whereas other localisation information will be sent periodically (e.g. Train Position Reports from a moving train unit every X seconds) and further localisation information may be sent in another (unpredictable) timely manner.

An unavailability of localisation information may have different causes and may result in different consequences in order to remain a safe representation in operating state. A basic working principle of APS is that a train unit is not supposed to move without a Movement Permission (see also chapter 4.3.3.1). In order to release a partial geometric extent of a Movement Permission due to a movement of a train unit, OA must identify this safe release by processing localisation information. In case that there is no localisation information available, the MP extent remains and will not be shortened.

The following table lists various degradations with different sets of localisation technologies deployed and describes resulting consequence in operating state as well as the resulting consequences for APS.

Localisation equipment	**Situation/Incident**	**Result in operating state**	**Consequence**
TTD only	TTD state lost	"Gap" in the geometric extent of a previous occupancy claim	Previously occupied TTD's remain occupied, MP extent will not be shortened Potentially enlargement of the MOB extension in the rear No Full-Supervision Movement Permission possible within that area.
TTD & TPR without safe train length	TPR localisation information unavailable or invalid at Start of Mission	Occupancy claim of train unit (MOB) based on TTD information only.	Manual process required in order to allocate the "free floating" MOB to the corresponding occupancy claim
	TPR localisation information unavailable while moving	• MOB rear end position always determined based on TTD information • MOB front position will be determined based on TTD information (as with TTD only) instead of based on TPR	MP Extent will be shortened based on TTD information
TTD & TPR with safe train length & integrity & always on	TPR localisation information unavailable while moving	1. MOB rear end position will remain unchanged at last known position 2. front end position will be determined based on TTD information 3. rear end position will be determined based on TTD information	MP extent will not be shortened any further than last known rear position MP extent will be shortened based on TTD information
	TPR localisation information unavailable while standstill	1. MOB position will remain unchanged at last known position 2. MOB extent (front and rear end position) will be enlarged according to underlying safety rules	MP extent will not be shortened any further than last known rear position
	Loss of integrity on a track section without TTD	• MOB front end position still determined based on TPR • MOB rear end position moved backward according to underlying safety rules OR MOB rear position remains at	Safety intervention by APS according to predefined rules MP extent will not be shortened

		last safely known position • MOB extent will expand • MP extent will not be cleared anymore by APS	

4.1.6 Delta

Applying a strictly geometrical representation of any object that occupies track sections and/or claims a track occupancy allows the optimum usage of track network capacity, particularly in areas where track sections between points or derailers are short and no TTD's are in place or vice versa when longer sections are covered with TTD's . Even though existing localisation technologies such as TTD systems are still needed for migration while not all train units are able to provide onboard, localisation information containing safe lengths and integrity, some geometric extent of already occupied TTD sections can be safely used for subsequent train movements. Strictly geometrical representation of any occupancy in a generic way allows a **high degree of technical independency from various existing and future localisation technologies**.

The handling of degraded situations (degraded modes) is based on a set of generic functions that allow each IM an **individual configuration** depending on the requirements and/or existing equipment (e.g. trackside sensors, handheld devices for track workers).

4.2 Occupancy claims NOT identifiable with localisation technologies

There are various causes of occupancy claims of a railway network within an Area of Control of an APS that cannot be identified by localisation technologies:

- Limitations in the usage of a track
- Routes that are reserved exclusively for a train unit movement by APS

4.2.1 Objectives and System Requirements

Objectives	System Requirements
APS@Interface with mobile devices in order to confirm the removal of a usage restriction area	$APS must support the confirmation of a URA removal from a mobile device $APS must ensure that URAs with safety relevance are not removed without adequate confirmation $APS must represent the operating state towards mobile devices in a fail-safe way
APS@Interface with mobile devices in order to represent safely the existence of a usage restriction area	$APS must represent any Map data in operating state in a fail-safe way $APS must represent any usage restriction in operating state in a fail-safe way $APS must represent the operating state towards mobile devices in a fail-safe way

APS@Only current occupancy claims and usage restrictions that forbid any movements shall hinder a movement	$APS shall base the granting or rejecting of requested movements on track occupancy claims and field element states $APS must consider all usage restriction conditions of the track segments claimed for a movement $APS must represent any track occupancy in a fail-safe way $APS must represent any usage restriction in a fail-safe way $APS shall be Safety Responsible for fail-safe granting movements to train units

4.2.2 Solution approach

The solution approach for the representation of a Movement Permission is considered in chapter 4.3.3.1, thus the focus of the following chapters lies in the management of Usage Restriction Areas.

4.2.2.1 Proposed representation of a Usage Restriction Area

Occupancy claims shall be represented in an abstract manner which is also true for occupancy claims that do not originate from a technical localisation equipment such as track closures for instance. Track closures or areas with reduced capabilities (e.g. reduced maximum speed, reduced maximum axle load) that will be generated by human actors or being derived from trackside sensors (e.g. avalanche detectors) are called Usage Restriction Areas (URA) hereafter. A URA shall be represented in the same generic manner as an occupancy claim in the operating state of APS: As a collection of track edge sections with the main difference that it can be fragmentary.

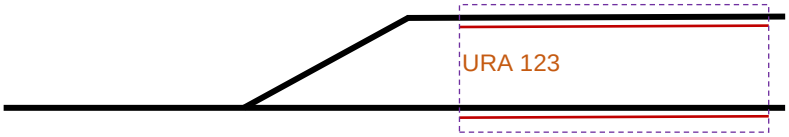

Figure 3: Example of a Usage Restriction covering multiple track sections

4.2.2.2 Proposed general working principle

Applying a URA in the operating state can be caused by two main reasons:

1. Planned (e.g. track maintenance)
2. Unplanned (e.g. avalanche or flooding happens “now”)

The solution concept foresees that planned URA’s are being requested from a) Plan Execution or b) by an APS user. In addition, APS will grant geometrical overlaps of multiple URA’s. (The basic rules APS applies, are being explained in chapter 4.3.3).

An unplanned URA can have two main characteristics:

- Requires **instant consideration** because it represents a current occupancy claim (e.g. avalanche detector, cracked track identified by track maintenance staff). This identified (unplanned) occupancy claim has to be processed by APS and represented in the operating state, regardless of existing occupancy claims (track occupancy, granted Movement Permission). In other words, this form of URA request must not be rejected by APS. To differentiate this particular form of URA request, it will be referred to as **URA Demand** hereafter.
- Requires **prompt consideration** because it represents an occupancy claim that will happen in close timely proximity (e.g. urgent maintenance work). This unplanned occupancy claim shall be requested to APS and checked if it can be granted and represented in the operating state from APS. This **URA**

Request can be rejected by APS, for instance when there is a geometric overlap with a granted Movement Permission.

Regardless of the form of application (planned, unplanned) a URA can have two operational reasons:

- Geometric extent of URA limits the utilisation of this track section e.g. due to a cracked track or a non-functioning point for instance but no track workers are on site
- Geometric extent of URA limits the utilisation of this extent because of the presence of track workers

To differentiate the two characteristics, the latter shall always be referenced from one or multiple 'Warning Area' (see chapter 4.4) if there are track workers on site.

When **removing a URA** it must always be considered that there may be track workers and/or machinery still on or close to the railway track within the geometric extent of this URA. In order to prevent the removal of an URA when there are still track workers within or close to this area, it is proposed that a URA can only be removed after a two-face commit: The final commit 'Yes, URA can be removed' shall be issued by the field responsible person of the construction area of this particular URA. It shall be possible to additionally verify the location with a handheld device carried by the field responsible person in order to reduce the hazard of granting the removal of a URA removal that is still used by another group of track workers – for instance on large construction areas.

Note: In case that there was a second construction area referenced to this URA, a second commit would be required from the second field responsible person, in charge of this particular Warning Area.

4.2.3 Problem description

Occupancy claims of the railway network that cannot be derived with existing nor future localisation technologies will need to be managed with the aid of manually supported processes. These will typically comprise of:

- Selection of one or multiple geometric extents of the track railway network, representing an area where occupancy claims will occur (e.g. for track maintenance work) or where track sections must not be used for train unit movements (e.g. cracked or broken rail)
- Such a reserved geometric extent must be communicated among all involved actors, for instance an operator in a central site and track workers in the field. Communication errors are a source for hazards (e.g. wrong track, wrong station, wrong timing) when applying and releasing a reserved geometric extent.

The aim of APS is to provide as much system functionality as possible to reduce the risk of human errors.

4.2.4 Migration

APS will offer the described functionality from the moment of deployment. Depending on an IM's needs, the configuration of APS will address any authorised user (actor) that will be able to request URA Demands. This may be a system user (e.g. OC connected to avalanche sensors) and/or a human user (e.g. the role dispatcher). Further on, it will be possible to configure users authorised to finally commit the removal of a URA (two-face commit) and from where (remote, on-site only).

Potential adaptations will be required in (standardising) graphical user interfaces and in managing URA's from a user's point of view. In today's signalling systems, usage restrictions are bound to preconfigured track sections (e.g. a route path, a mainline track, a station track) and with APS, there may be supporting features that allow a user to select quickly e.g. a set of track sections in order to place a URA but a URA can "start" and "end" at any location on the railway topology and comprise multiple sections.

4.2.5 Degraded modes

Situation	Result in operating state	Resulting Consequence	Mitigation
URA has been requested by mistake	URA represented in operating state	URA causes unwanted impacts to operation (e.g. max speed)	Remove URA manually, see also row '*On-site commit for URA removing not possible*'

URA demand issued due to failure	URA represented in operating state URA extent may overlap previously granted MP	Granting of later MP not possible or only with limitations (e.g. maximum speed limited) Depending on the URA type and location an existing MP may need to be modified (e.g. shortened or further restricted)	Sensor/s will need to be reset or checked on-site Eventual risk mitigation measures
On-site commit for URA removing not possible	URA represented in operating state	Verification of URA location not possible in the required timely manner, because there is no authorised field responsible person on or close to this URA location	Individual IM process, utilising one or multiple functional building blocks from APS Example: On-site commit not required when no Warning Area has been assigned to this URA, hence URA can be removed centrally
URA has been demanded over granted MP extent	URA represented in operating state	Potential hazard for train unit that moves within MP extent Depending on the URA type the existing MP must be modified (e.g. shortened or further restricted)	See chapter 4.3.4.1

4.2.6 Delta

The described additional functionality for track occupancy claims not identifiable by localisation technologies represent a major **improvement for track worker safety**.

The handling of degraded situations (degraded modes) is based on a set of generic functions that allow each IM an **individual configuration** depending on the requirements and/or existing equipment (e.g. trackside sensors, handheld devices for track workers).

4.3 Safety Checks

4.3.1 Objectives and System Requirements

Objectives	System Requirements
APS@Allow safe movements also when train characteristic are unknown	$APS shall not prevent a movement of a train unit with unknown characteristics $APS must comply to defined safety conditions
APS@Allow still safe best production under circumstance of reduced availability of reliable information	$APS shall allow movements under specific conditions, when localisation information becomes unavailable $APS shall allow movements under specific conditions, when states of switchable field elements become unavailable $APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back $APS must not grant a movement when safety conditions are violated $APS must be able to identify safety condition violations $APS must take one or multiple safety measures when a safety condition violation is identified $APS must support the configuration of safety conditions according to an IM's needs $APS shall support the transfer of Safety Responsibility in an automatic way
APS@Build a system that does not consider in its logic operational implications but only checks for safe operation (separate business logic and safety logic)	$APS shall not limit the start and end of movements to specific positions in the Area of Control $APS shall not consider any operational consequence when granting movements but solely if the movement is safe
APS@Consider speed limitations only on the specific geometric extent	$APS shall prevent a train movement from exceeding a speed limitation within its defined geometric extent
APS@Consider train specific characteristics when granting movements	$APS shall prevent movements when safely known train characteristics violate usage restrictions defined in the usage restrictions of the track section claimed for this movement
APS@Grant movements considering the operational needed safety level and the possible risk mitigation measures	$An IM shall have the possibility to configure safety conditions according to its requirements and regulations $APS shall consider the safety conditions configured by an IM according to its requirements and regulations

APS@Ensure safeguarding of all movements on railway tracks within a geographical region	$APS shall not limit the start and end of movements to specific positions in the Area of Control $APS shall not prevent a movement of a train unit with unknown characteristics $APS must comply to defined safety conditions $APS shall allow movements under specific conditions, when localisation information becomes unavailable $APS shall allow movements under specific conditions, when states of switchable field elements become unavailable $APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back $APS shall allow the geometric overlap of two route paths complying to the defined safety conditions
APS@Identify safety rule violations during runtime and initiate safety measures in order to mitigate safety hazards	$Each safety condition APS checks shall be unambiguously specified $Each safety condition violation, identified by APS, shall be unambiguously specified $Each safety measure, APS and its resulting safety condition cause, shall be unambiguously specified $An IM shall have the possibility to configure parameters for each safety condition, each safety condition violation and each safety measure according to its requirements and regulations $APS shall consider parameters for each safety condition, each safety condition violation and each safety measure configured by an IM according to its requirements and regulations
APS@Implement a strict object aggregation for enabling of usage of different information sources and simplification of interfaces within the system and future adjacent systems (avoid the need to implement a logic knowing exact behaviour of interfacing parts)	$All APS interfaces must be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact and testable way $The behaviour of the individual APS components should be formally specified when required by formal validation $Ensure clear layering for transport, marshalling and application model $APS shall encapsulate translation logic from processing logic $APS shall implement a strict object aggregation, based on abstract concepts
APS@Implement full supervision of all movements, also shunting	$APS shall enable operation without the need of lineside signalling system $APS shall not limit the start and end of movements to specific positions in the Area of Control $APS shall not prevent a movement of a train unit with unknown characteristics $APS shall implement full supervision of shunting movements

APS@Presuppose the existence of a radio-based Train Control System (ETCS) assuming a continuous communication connection to each train on-board unit	$APS support different ETCS system versions within the same APS Area of Control $APS shall provide interfaces that are compliant to the TSI CCS $APS shall consider to handle trains with continuous communication connection
APS@Provide measures to reduce hazard when safety rule violation is identified	$APS must be able to identify safety condition violations $APS must take one or multiple safety measures when a safety condition violation is identified $APS must prevent collisions $APS must prevent derailments
APS@Provide real-time operating state	$APS must represent any track occupancy in a fail-safe way $APS must represent any usage restriction in a fail-safe way $APS must represent in real-time all movable objects within its AoC in a fail-safe way $APS must represent in real-time all granted movements in a fail-safe way $APS must represent in real-time the current state of a switchable field element in a fail -safe way
APS@Regard Map data as fail safe	$APS shall consider the provided Map Data as fail safe
APS@Support FRMCS for communication between track side and onboard	$APS shall support GSM-R for a transition period $APS shall support FRMCS-technology based communication technology for all communication purposes between onboard and trackside $Ensure clear layering for transport, marshalling and application model
APS@Provide operating state towards mobile devices	$APS must represent any track occupancy in a fail-safe way $APS must represent any usage restriction in a fail-safe way $APS must represent in real-time all granted movements in a fail-safe way $APS must represent in real-time the current state of a switchable field element in a fail-safe way $APS must represent the operating state towards mobile devices in a fail-safe way
APS@Publish safety rules and config data towards operational level	$APS shall make the generic safety rules and the specific configuration data of the function make available for the operational level
APS@Support automated coupling	$An IM shall have the possibility to configure parameters for each safety condition, each safety condition violation and each safety measure according to its requirements and regulations
APS@Support different ATO levels (GoA1 – GoA4)	$APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back $APS shall support the transfer of Safety Responsibility in an automatic way

4.3.2 Problem description

Today's interlocking systems have historically evolved. Many risk mitigation functionalities have been introduced over time. These have been derived from a variety of sources such as for instance new legislations, limitations of technical options and a demand for higher degree of automation. Differences in operational and legislative rules between shunting and train movements required either different rules and configuration implementations or at least adaptations of previously existing rules and configurations. The introduction of new and/or additional safety systems such as ETCS required additional project engineering configuration and implementation efforts partially because existing engineering and/or configuration data could not be reused because of a lack of compatibility and/or inexistence (except as configuration in one interlocking system). Dependency between life cycles is therefore high (for instance an IM cannot replace an end of life interlocking without adapting the interconnected RBC).

The reaction on safety condition violation is reduced to change the driving term on a light signal to 'Stop', meaning that a train unit cannot be stopped before it reaches this particular light signal. Moreover, it cannot be stopped once the train passes the signal showing a stop aspect. Depending on the integration depths, when using radio based ETCS, there may be the possibility to send an emergency stop command to the particular train unit.

4.3.3 Solution approach

Core Principle 3 – No operational and processual functionality

A major objective of APS is that there shall be no functionality in APS that covers with operational or processual requirements (e.g. dead-lock prevention, conflict resolving, operational optimisation of infrastructural usage). The APS' range of functions shall be kept to an absolute minimum to enable minimised approval efforts and maximum independency from changes from interconnected subsystems (life cycle, new/changed Field Elements/technologies). Any functionality not declared as safety critical shall be realised out of scope from APS. (Note: There will be safety relevant functionalities within the scope of RCA, not realised by APS but in other components such as Object Controller for instance.)

Core Principle 4 – Deploy Generic Safety Checks

No site-specific configuration of the safety logic of APS is needed because APS' generic safety conditions shall be applied to any railway topology characteristic within the Area of Control. As described in chapter 2.1, the unified logical representation of the railway network topology in operating state and its occupancy claims, states are based on a Node-Edge model where edges have – among other attributes – a geometric extent, a length. Each request sent to APS can contain the following information:

- A geometric extent in form of Track Edge Sections (e.g. Movement Permission, Usage Restriction)
- A reference to an object in the Map Data that has a geometric extent (e.g. Drive Protection Section Group, Drive Protection Section)

In this concept, a proposal is made in order to represent requests and its results after performing safety checks, which is described in the subchapter hereafter.

4.3.3.1 Proposed representation of switchable Field Elements

A set of field elements influences through their positioning the drivability of a route path. A generalisation of all such field elements shall be achieved through abstraction in the Map Data, allowing the route path to any location on the Track Edge to be set without regard to what kind of Field Element this path claims. The abstract object representation in the Map Data represents each field element that can change its state as so-called **Drive Protection Section Group** (DPS Group). Each DPS Group consists of one or multiple **Drive Protections Sections** (DPS).

Example: A single point is being represented with two DPS (DPS_1, DPS_2). Both DPS are modelled as a section on a Track Edge and represent the moving parts, their trafficability state and the interdependencies between the two DPS (in case of a single point, it will be a NAND interdependency). Possible DPS states shall be 'trafficable' and 'not trafficable'.

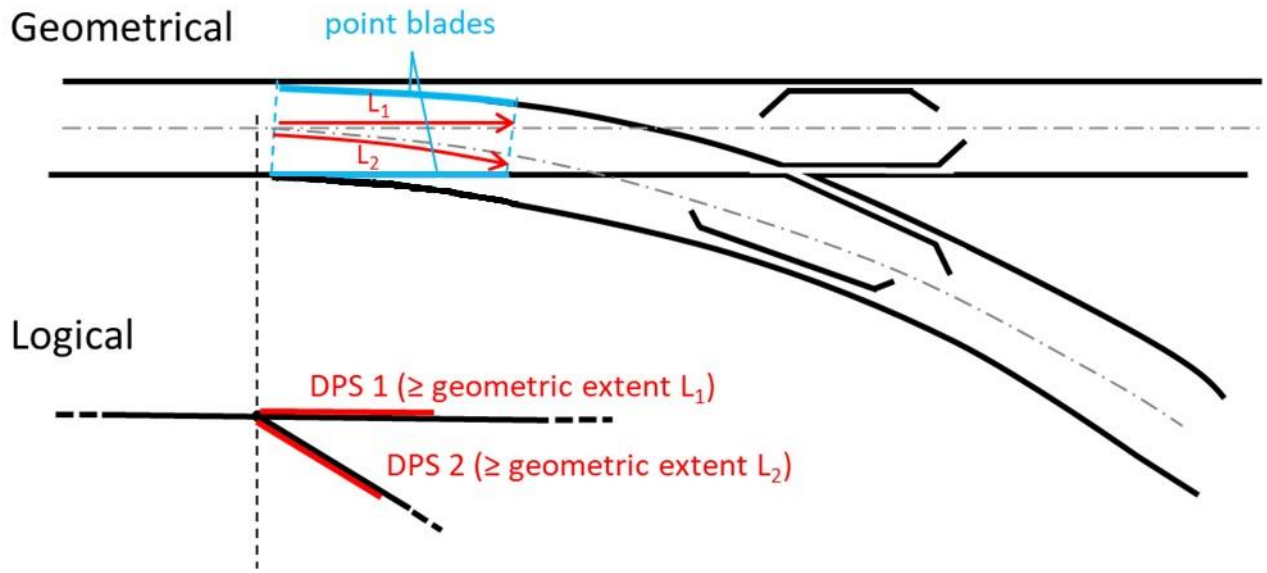

Figure 4: Representation of Drive Protection Sections (DPS) of a Single Point

Allocation Section

There are track sections where the minimum distance in between two track axes is undercut (e.g. 3.6 m depending on the specific clearance gauge and reference profile of the train) which would cause a collision in between two intersecting train units. Typical examples of such sections are areas within:

- A single point
- A double slip point
- A crossing
- Multi-gauge tracks
- Straight sections where track axis undercut the minimum distance

This concept proposes that each track section where this distance is not adhered to is represented explicitly as so-called **Allocation Section as part of Map Data**. In other words, Allocation Sections are part of the engineering process when preparing Map Data.

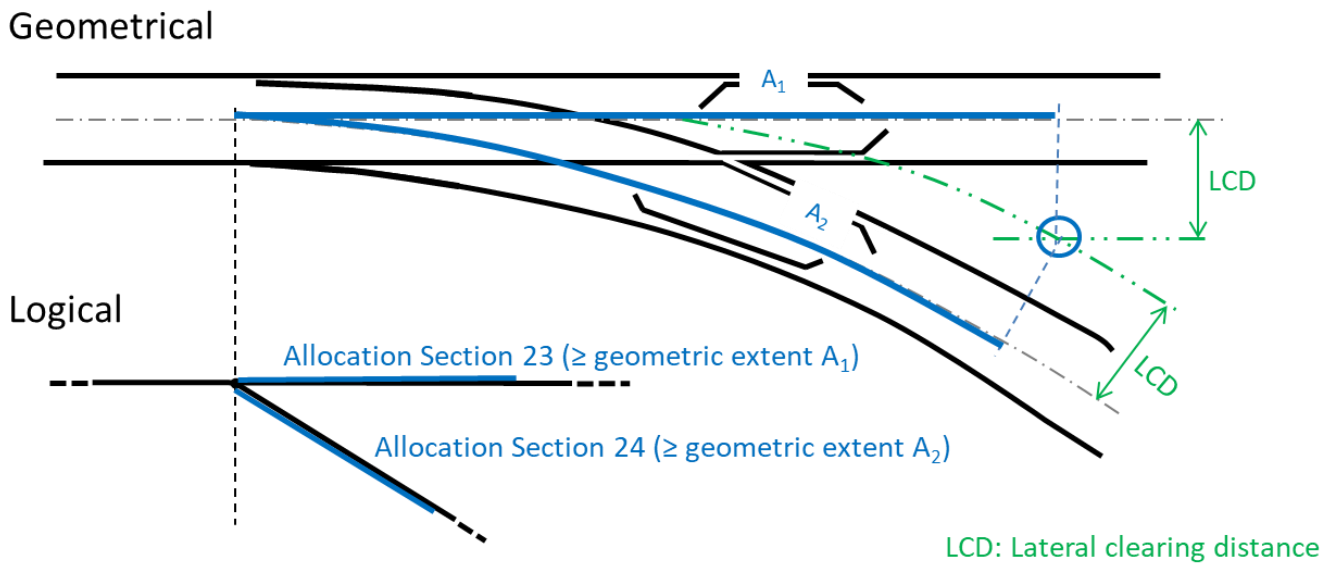

Figure 5: Representation of Allocation Sections of a single point

Allocation sections will allow APS to identify any track section for which protective measures must be in place according to the defined safety conditions.

4.3.3.2 Proposed representation of a requested and secured route path

This concept proposes to represent a request and a representation for and of a route path for a train unit movement as a so-called **Movement Permission**. The characteristics of a Movement Permission are:

- Unambiguous description, based on Node-Edge model of the Map Data
- Comprises
  - A Movement Permission extent (is the route path to be secured for a train unit's movement)
  - An optional* Risk Buffer (a safety margin as continuation of the MP extent in case a train exceeds its movement beyond the end of its MP extent)
  - Optional** Allocation Sections (description of areas for enabling check conditions concerning clearance gauge at Field Elements)
  - Optional** Risk Path(s) (safety area towards a location for mitigation of possibility of a flank collision)

*) Optional Risk Buffer: Risk Buffer may not be required by all IM's and/or not in all operational scenarios. Example: One IM requires Risk Buffer when approaching speed exceeds 40 km/h.

**) Optional Risk Path: As with Risk Buffer, Risk Path may not be required by all IM's and/or not in all operational situations. Example: One IM requires Risk Path only when train unit speed is higher than 80km/h.

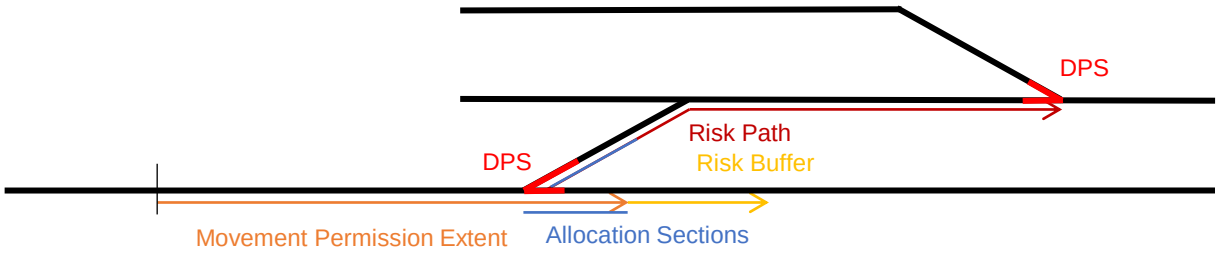

Figure 6: Composition of a Movement Permission

Note: Figure 6 depicts already the differences between a Movement Permission Extent and an ETCS Movement Authority.

4.3.3.3 Proposed general working principle

After having received a request to grant a movement of a train unit on a track path, APS will check if all defined safety conditions are being fulfilled or not. If one or multiple safety conditions are violated, this request will be rejected by APS, otherwise the request will be granted.

A safety condition describes a condition that must be fulfilled when geometrically overlapping a request with the identical geometrical extent in the operating state. Example: “Partial or full geometrical overlap of an MP extent with a Drive Protection Section showing state ‘not trafficable” is not allowed.” All safety conditions from APS must also be known to the requesting plan execution functionality (performed by PE) in order to successfully send requests towards APS.

Note: Safety Conditions refer to geometric overlaps between objects that use the identical Map Data as PE, hence no additional or further interpretation of these safety conditions is being required from the side of PE.

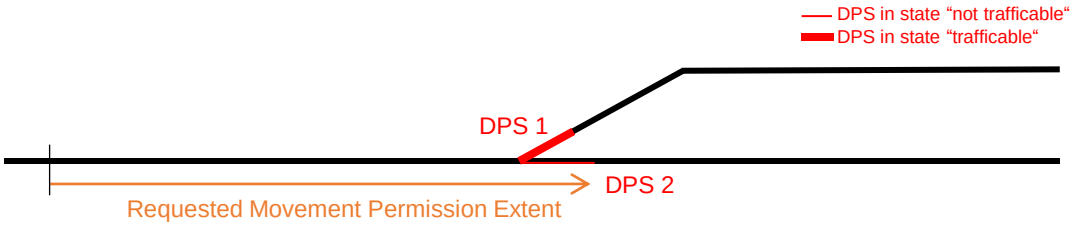

Figure 7: Geometric Overlap of MP Request in current operating state resulting in rejecting the MP Request

This working principle requires that each geometric extent of the railway network that can change its state (field elements such as e.g. points, lifting bridges, derailers) must be in the required state prior to any Movement Permission request. To summarise, APS must check two types of requests:

- State change requests of DPSs (abstraction of switchable field elements) that either determine a route path (e.g. points, lifting bridges) or protect a route path from side collisions (e.g. flank protecting element, level crossing)
- Occupancy claim requests in the form of Movement Permission requests or Usage Restriction requests

Depending on the type of a granted request APS will:

- State Change Request: Command a state change towards Object Controller (OC)
- Occupancy Claim: Represent the granted occupancy claim in operating state and in case of a Movement Permission: Communicate additionally the granted Movement Permission in the required technology (translate in Device Abstraction Layer) to the train unit

Note: The current state of a field element will be represented in operating state after a state change has been identified by APS.

In the following sub-chapters, the basic rule sets are being explained in a general manner. Further details can be found in the APS Detail Concept documentation which will be created at a later stage.

Note: With reference to chapter 3.1, it is proposed, that each set of safety conditions or each safety condition shall be encapsulated in so-called minimal functional blocks. Characteristic of a minimal functional block is that it processes a minimal set of input data and its output is always binary. Each functional block can be safety

assured and the combination of N minimal functional blocks will result in a functionality (e.g. implemented as a component) that will be safe without an additional safety assurance.

4.3.3.4 Route Setting and Protection

Prior to protect a route for a safe movement, the route needs to be set to fulfil the following main conditions:

- Set all switchable field elements (e.g. points, lift bridges) within the geometric extent of the Movement Permission to be requested in the required state
- Set all required protective measures (e.g. flank protection set, level crossing set)

Afterwards, the following checks need to be performed for route protection:

- Is the route clear of any occupancy claim and/or are occupancy claim limitations being respected?
- Are all field elements in the route path secured against state changes?

Identify the State of a switchable Field Element

States and State changes of switchable field elements are being send to APS via Object Controller and translated in the Device Abstraction Layer into a generic representation (see chapter 4.3.3.1) of Drive Protection Section (DPS).

APS will represent each received state and state change for each DPS immediately in its operating state, regardless of eventual occupancy claims in the operating state.

Example: A point has been set and allocated to a Movement Permission overlapping that point in the moment of granting that Movement Permission. While a movement within this MP happens, the point loses its monitoring and therefore its current state becomes 'Unknown'. This situation must be represented as fast as possible in operating state to perform eventual safety measures and to eventually redirect the next train run.

Note: Redirecting is an operational aspect (rescheduling), handled outside of the scope of APS.

Set switchable Field Element in required State

Each DPS within the Movement Permission to be requested must be set in its required state prior to an MP Request. Such a request to change a state of a DPS is called DPS Request hereafter. Each DPS Request will be checked by APS if the request fulfils all defined safety conditions. A DPS state change is basically allowed when its geometric extent does neither partially nor fully geometrically overlap in the operating state with

- A Movable Object
- A Movement Permission Extent
- A Risk Path
- A Risk Buffer (configurable if checked or not)
- A specific type of Usage Restriction Area (URA)

Route Clear Checking

When receiving an MP request, the following occupancy claims within the requested geometric extent of the MP may exist in operating state:

- Another previously granted Movement Permission
- One or multiple previously granted Usage Restriction Areas
- One or multiple MOB

APS will grant this MP request under the following main conditions:

- No partial or full geometric overlap with a MOB except the MOB that the MP refers to

    - Exception: Partial overlap allowed under defined conditions in order to join two train units (assuming they are not always reporting) or at the Start of Mission (SoM; procedure for start-up of an ETCS train) for instance
- No partial or full geometric overlap of the requested MP extent with another MP extent
    - Exception: Partial overlap allowed under defined conditions in order to join two train units for instance
- No partial or full geometric overlap of the risk buffer with another risk buffer if not allowed (configurable)
- No partial or full geometric overlap of the requested Risk Path extent with another MP extent or Risk Path extent
- No partial or full geometric overlap of MP Extent with a geometric extent of a URA whose limitations are violated
- There is no train characteristic* that violates a movement condition of the MP extent
- No violation of Route Protection conditions (see paragraph hereafter)

) Note to Train Characteristic: It is foreseen to process future train characteristics when granting a Movement permission. Train characteristics may be: axle load, breaking capability, dangerous good,** loading gauge. Nevertheless, standardisation (e.g. in scope of Digitally Automated Coupling) and technical discussions are still ongoing and therefore further clarification is expected in the future*

Route Protection

To protect a route, the following safety conditions must be met:

- Movement Conditions in the requested Movement Permission do not violate usage conditions of the underlying railway network topology section
    - Movement conditions such as speed, movement mode (describes which actor has the Safety Responsibility during a movement, e.g. for ETCS this would be translated into a ETCS MA Mode)
- DPS in correct state
    - all DPS within the geometric extent of the MP extent must be in the required state
    - all DPS within the geometric extent of the Risk Buffer extent must be in the required state (configurable if applicable or not)
    - all DPS within the geometric extent of the Risk Path extent must be in the required state (configurable if applicable or not)
- DPS states protected from changing
    - all DPS states within the geometric extent of the MP extent must be protected against any change
    - all DPS states within the geometric extent of the Risk Buffer extent must be protected against any change (configurable if applicable or not)
    - all DPS states within the geometric extent of the Risk Path extent must be protected against any change

If none of the safety conditions and checks listed above under ‘Route Clear Checking’ is violated, APS will grant the Movement Permission request. This granted MP Request shall be instantly represented in the operating state before communicating it towards the train unit.

Communicating a Granted Movement Permission

After a granted MP Request is successfully represented in the operating state, the MP is sent towards Device Transaction Layer where it will be translated into e.g. an ETCS Movement Authority. In order to do so, the responsible subsystem must be in possession of:

- MAP Data to be able to map geometric extents into location reference-based distance information

- additional topological data containing the location references used for communication with the train (e.g. balises) in order to calculate the geometric distance from the last relevant balise group until the begin and end of a geometric extent
- Additional topological data not contained in the MP Request but required to submit a Movement Authority such as track conditions, gradient and linking information

4.3.3.5 Automatic Route Releasing

Even though APS will neither grant Movement Permissions nor request state changes* of field elements without being explicitly triggered by Plan Execution, it is going to automatically release route sections that have been traversed by a moving train unit (automatic partial release of a granted Movement Permission Extent) so that these track sections can be reused for other movements as soon as possible.

**) Annotation: APS may demand state changes as reaction of recognised incidents e.g. a runaway vehicle. This is to be defined in the course of the project.*

APS will do so by identifying the safe rear of a train unit according to its aggregated representation of the occupancy claim (MOB) in the operating state. As described in chapter 4.1.3, the safe identification of a rear end depends on the localisation technologies available; utilising TTD equipment, the rear end will be "dictated" from the geometric extent of a TTD section, utilising (future) safe train length and integrity information from ETCS onboard will allow to partially release granted MP extents as soon as a safe rear information has been received, processed and represented in operating state.

4.3.3.6 Migration

The biggest impact compared to today's signalling systems will be the move towards the free choice of any extent of the railway network for movements and usage restrictions. This will influence existing systems such as planning or dispatching systems. Nowadays, spot locations such as light signals or their "location of impact" are used to e.g. calculate an absolute point in time where a train run is supposed to arrive or depart.

The circumstances of cab signalling in combination with no more requiring fixed blocks / track sections (and therefore no light signals at spot locations) will most likely have consequences on today's operational rules, processes and standards for managing standard scenarios and degraded modes for all involved actors.

To allow a smooth transition and migration towards this operational environment, the proposed concept allows a variety of adaptations to today's signalling environment. Examples:

- Fixed blocks or preconfigured track sections ("virtual signals") may be added in Map Data in order to support existing signalling systems, existing graphical representations and so on that will be consumed by PE in order to request Movement Permissions according to these preconfigured track sections.

When introducing APS (or the RCA approach to be precise), it is a big advantage that there is a unified and common data source in form of Map Data in combination with the proposed usage of all involved SubSys, including APS. From an APS perspective, there is no longer the need to do separate project engineering efforts for the "route protection" and "the train control" side.

4.3.4 Degraded modes

Nr.	Situation	Result in operating state	Resulting Consequence	Mitigation
1	DPS not in required state when requesting an MP	None (DPS reflects current state)	MP request rejected	Request DPS state change and request MP after DPS state is in correct state in operating state
2	DPS not in required state after granting a DPS request	1. DPS reflects current state 2. Difference in between granted DPS state	1. MP cannot be requested (would lead to reject of MP request)	Resend DPS state change demand within a defined time frame (DPS state change will eventually occur)

		change request and current DPS state	2. Current DPS state will potentially change 3. Failure revelation	DPS state change demand command with a maximum time to life capability to prevent delayed ("forgotten") state changes Chose different route for MP (rescheduled from TMS, PE) Movement over this DPS possible under special conditions, see "*DPS state lost or unknown despite correct position of field element, no MP granted over it*"
3	DPS state lost or unknown, no MP granted over it	DPS is not trafficable	1. DPS cannot be used at all for an MP, or 2. DPS can be used for an MP with restricted conditions 3. Failure revelation	Define DPS state manually after it has been locally assured that field element cannot change the manually identified state. OC will not accept any state change commands as long as this manually defined state is present, regardless if field element state could be changed again.

4.3.4.1 Identifying safety condition violation after granting an MP

In the previous chapters, safety checks have been described that take place on the basis of a request. Additional functionality will be necessary to identify safety condition violations after a Movement Permission has been granted and communicated. Such safety condition violations may occur for instance when:

- A run-away vehicle moves without an MP and can collide with another train unit or human beings on or close to the track
- A train unit with a granted Movement Permission overruns the end of its Movement Permission due to braking failure
- An uncontrolled DPS State change within a granted Movement Permission

Common to all cases mentioned is the fact that they are a potential hazard for any safe movement (or even a train unit at standstill). Hence, identification of safety condition violation is a functionality required from APS. Performing one or multiple reactions in order to reduce the risks caused by an identified hazard is also a required functionality from APS.

At this stage of the project, some scenarios or use cases of hazards to be identified and its mitigation actions were discovered together with IM's:

Nr.	**Scenario**	**Required identification of**	**Possible mitigation action/s by APS**
1	DPS loses its state after granting an MP over it	DPS state change will be reflected in operating state	APS shall ensure that the train is stopped in front of the DPS if the train has not yet passed this DPS
2	MOB leaves its MP extent	• Identify if the MOB extent leaves its corresponding MP extent (irrelevant if partially or fully)	• try to stop moving train unit

		• Identify the direction in which the MOB extent leaves its MP extent • Identify the path which the runaway train unit will follow based on the current position, the current direction and the current DPS states along this path for x Meters (x shall be configured by IM) • DPS states other than fully drivable shall not be considered	• Prevent other movements from colliding with the runaway vehicle • If existing along the identified path: Demand DPS state changes for level crossings to prevent collisions between road traffic and the runaway vehicle
3	MOB leaves its stop position and starts moving	*Note: Depends on the final implementation decisions: Does a still standing MOB keep its MP or will the MP be removed?* • MOB starts moving without having an MP • As for scenario #2	• As for scenario #2

4.3.5 Delta

What drops with APS	**What comes along with APS**
No multiple sources of basic Map Data ("topology data")	The Map Data is based on a standardised model that represents the physical railway network in form of a logical Node-Edge Model. For safety relevant systems, each version of a topology data set will be validated prior to its use by safety relevant system. For non-safety relevant systems, the same version of topology data set shall be used but may be completed by additional topology data required. In order to assure a form of synchrony between all consumers of a version of railway network topology data set, an overarching mechanism is proposed. Utilising the identical version of a topology data set among all involved systems allows: • Common frame of reference • Common interface language to describe • Routes along the railway network • Spot location positions and geometrical extent (e.g. for track occupying elements, for positioning of trackside elements along the railway track) • No or less interpretation effort in between systems • Same information content for all systems involved
There will be no preconfigured track routes including all its dependencies such as light signals, point positions etc.	Each and every movement within a track area, controlled by APS will be requested by the overlying systems (PE) in form of a track precise route, represented as uninterrupted sequence of logical track sections. Such a requested movement is named 'Movement Permission Request'. The requesting system must make sure that safety related rules are not being violated in order to prevent a rejection from APS. Examples for a safety related rule: • A point must be in the correct position prior to a Movement Permission request. Hence the requesting system must request that correct point position prior to requesting a Movement Permission.

	• Possible flank protection measures required in order to safely pass e.g. a point must be set and requested before requesting a Movement Permission Reduction of the number and complexity of checking rules to a minimum number of basic (generic) rules for the longest possible life cycle and implementation of business logic on the side of the requesting systems.
There will be no differentiation between train run and shunting movements.	Generic rules will be applied to any form of movements. Variations (e.g. different distances between two moving trains, flank protection aspects, etc.) are derived from rules based on configuration parameters that are valid for at least one entire APS area of control.
No support for light signals on static spot locations with the exception of the support of light signals at APS area of control borders to/from existing legacy interlocking systems	Movement commands towards the train driver and/or automated onboard systems (GoA2/3/4) are being sent to a specific train unit, utilising ETCS standards.
No geographical and site-specific configuration data for safety related checks (e.g. no fixed block sections necessary)	The geometric extent of a Movement Permission can be freely defined by the requesting system. APS does not check if a request is operationally reasonable but if no safety rule is violated. Note: Geographical and/or site-specific rules and/or dependencies that are operationally necessary are still possible on the side of the requesting system such as PE for instance.

4.4 Managing Warning Areas

4.4.1 Objectives and System Requirements

Objectives	System Requirements
APS@Enable automatic warning areas and movement limitations without the need for manual interactions	$APS must consider Warning Areas when granting movements $APS must communicate with Warning Systems in order to send warnings and to receive acknowledgements $APS must make sure that prior to any movement within a Warning Area, an onsite warning – according to defined conditions - will be issued
APS@Prevent granting a movement over predefined geometrical areas without prior warnings to track workers	$Before granting a movement, APS must secure that the configured minimum pre-warning time is not violated $Before granting a movement, APS must secure that the configured maximum pre-warning time is not violated $An IM shall have the possibility to configure the minimum and maximum pre-warning time $APS must ensure that the Warning System has confirmed the Warning Command by APS before granting a movement $APS must be able to update a previously issued Warning Command

APS@Provide functionality to define geometrical extents for warning areas within the Area of Control	$APS shall provide a functionality to create, change and delete geometric extents in operating state, representing a Warning Area $APS shall support the creation, change and deletion of a Warning Area to the authorised actors Plan Execution and human beings $APS must prevent that Warning Areas geometrically overlap
APS@Support interfacing with existing warning systems for track workers	$APS must support the transmission of a Warning Command to a Warning System in the field $APS must support the reception of a Warning Command acknowledgement from the Warning System
APS@Support safe entry and exit from a construction site or maintenance location for track worker and machinery	$APS must issue an individual Warning Command for each individual train unit $APS must be able to issue Warning Commands in case of an identified runaway vehicle that may enter a working area $APS must be able to communicate the geometric extent of a Warning Area to a Warning System

4.4.2 Problem description

Warning Areas shall be geometric extents on the railway network topology where track workers within this area need to be warned from an approaching train unit prior to the entering of a train unit into this area to allow enough time to leave their particular area. A warning signal towards track workers is issued typically from a locally installed warning system in form of an acoustic and visual warning signal within and/or along a warning area. There is typically a minimal and maximal time frame where such warnings shall be released prior to an approaching train unit, called minimal and maximal pre-warning time hereafter. This time depends on many parameters too. There are some timely challenges when issuing warnings on construction sites.

Example 1: A train unit comes to a (planned) stop before crossing a Warning Area. The challenge in this scenario is the point in time for issuing the warning signal on-site that complies to the defined (configurable) conditions of the minimal and maximal pre-warning time because the train unit may depart on (planned) time or later (e.g. door malfunction). Regardless, whether the train starts on time or delayed, the MP needs to be issued before the on-site warning signal can be issued in order to comply with the minimal and maximal pre-warning time requirements of the specific IM.

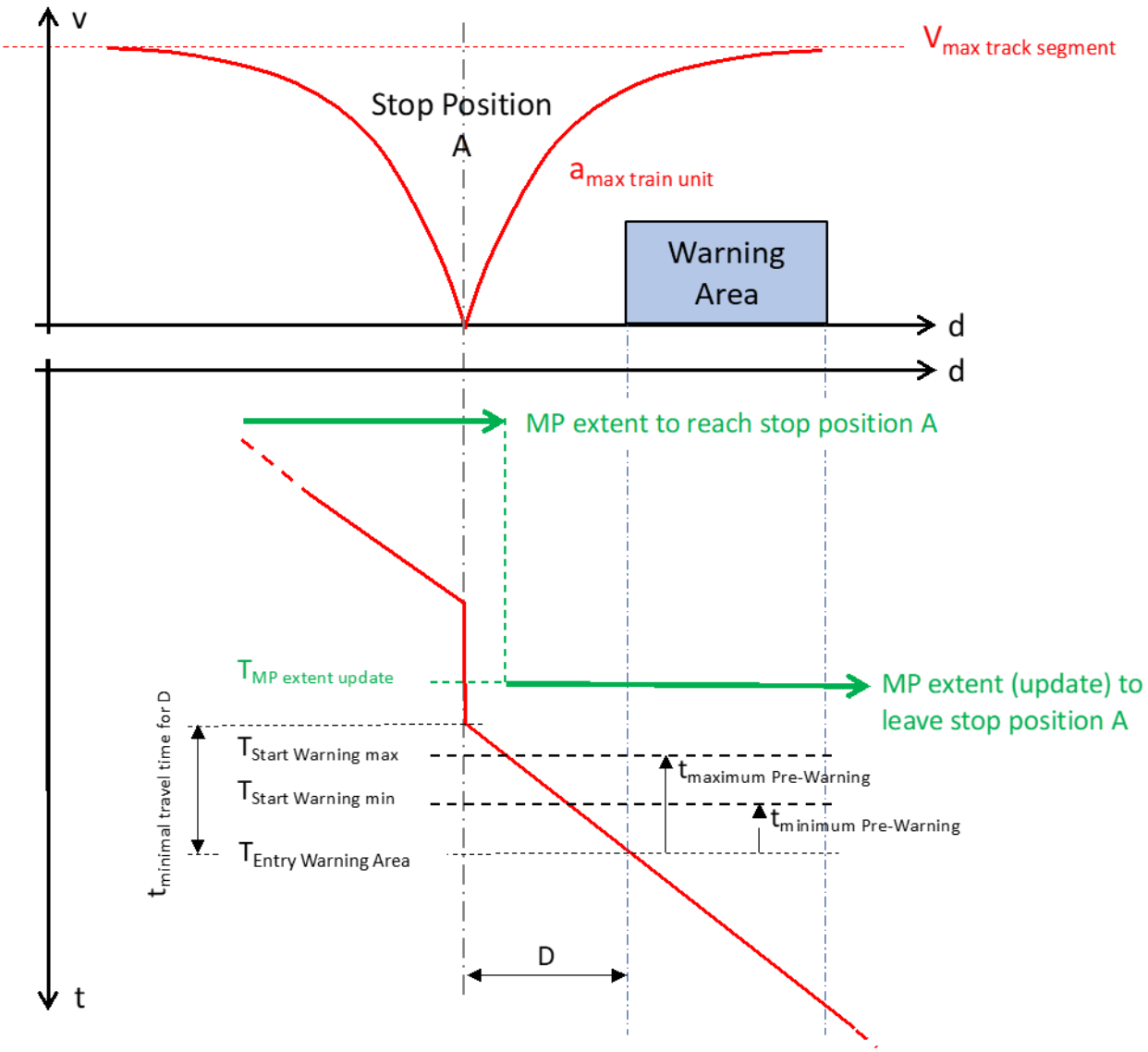

Figure 8: Stop before entering a Warning Area

Conclusion 1: Considering the basic working principle in chapter 4.3.3.3 that before an MP can be granted, all states from field elements need to be in the correct position, one could argue that Warnings would also be part of the (granting) conditions. This was possible when maximum allowed speeds in the MP would be lowered to the point where the minimal travelling time is always higher than maximal pre-warning time. This approach, however, would conflict with the business target *'#Capacity shall in terms of CCS only be dominated by the abilities of the trains and the physical track layout*'. Hence, the solution requires some independence between the points in time of a) granting an MP and b) releasing a warning signal for a particular movement of a train unit.

In order to calculate the point in time for releasing the on-site warning signal, the track network geometry plus the speed profile of the granted Movement Permission needs to be known to the corresponding function. This information is part of the (granted) Movement Permission Extent.

Example 2: A train unit with a (very) flat breaking curve (e.g. a freight train) will pass a Warning Area. This requires the granting of an overlapping MP extent with this Warning Area prior to the point in time when the Warning needs to be issued.

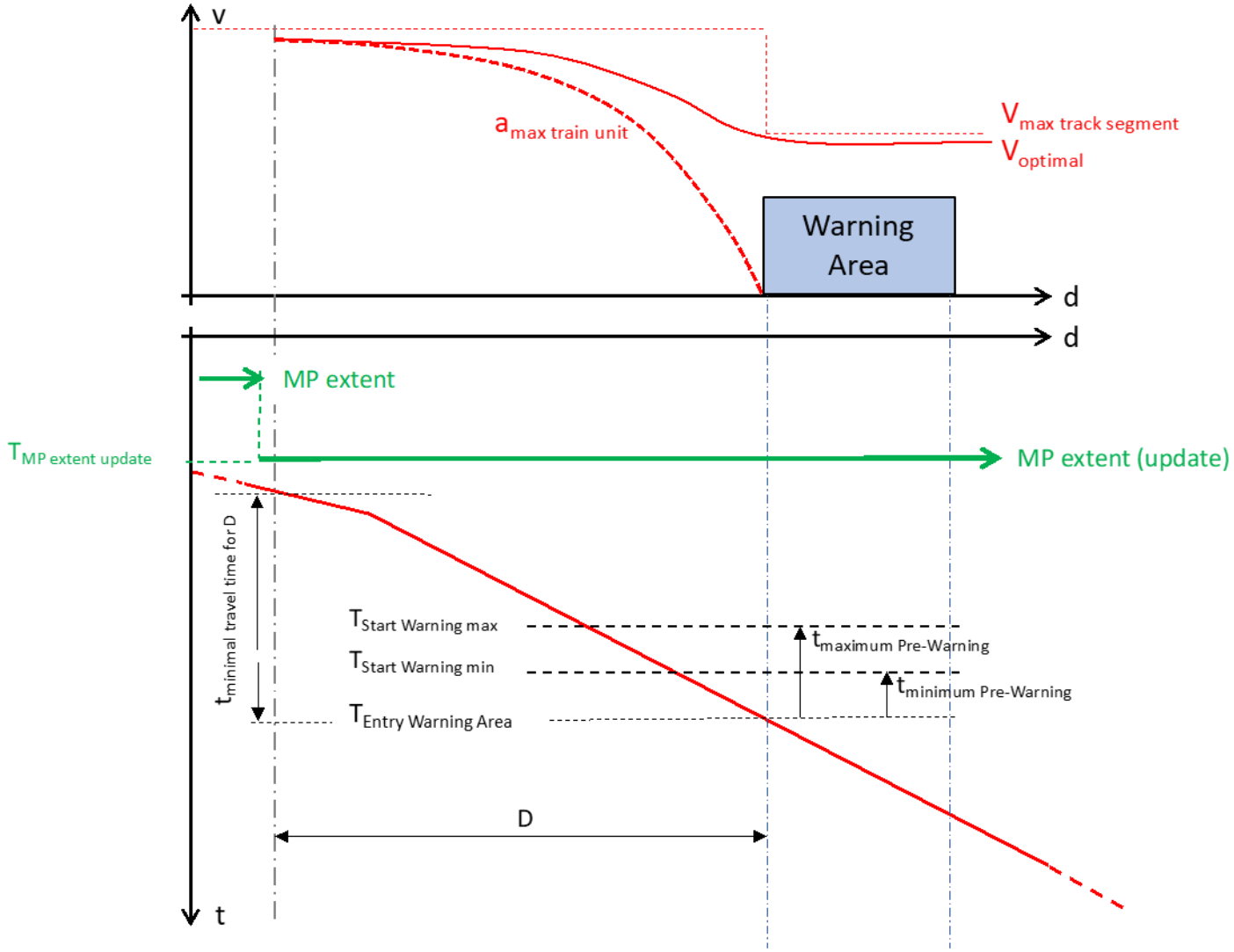

Figure 9: Weak braking power requires the early existence of an MP (extent) within a Warning Area

Conclusion 2: A solution that requires the issuing of an on-site warning signal prior to granting a Movement Permission is not feasible. Hence, a solution is required where the Warning System will fail-safe output an on-site warning signal independent of the point in time when a Movement Permission is being granted by APS over this Warning Area.

4.4.3 Solution approach

The purpose of a Warning Area is to warn track workers by usage of Warning Systems on-site within the geometric extent* of this Warning Area in case that defined conditions are being met when a geometric overlap between a warning area and a Movement Permission exists. When conditions are met, a Warning Command shall be issued from APS to the corresponding Warning System. The Warning system shall receive this Warning Command and issue a warning on site (acoustic, audible, other) according to the defined pre-warning time spans.

The Warning device itself is out of scope of APS but will have an interface from/to APS to receive Warning Commands from APS and to send Warning Command acknowledgments back to APS so that granting an MP request becomes possible for APS. Warning Areas shall not geometrically overlap to prevent Warning releases from two different Warning Systems for the same geographic area.

Additionally, a Warning Area allows to identify locations of mobile localisation devices (worn by track workers) within or approaching this area and to issue warnings when configurable conditions are being met. These

warning conditions are to be configured as part of the Warning System configuration and is out of scope of APS.

**) Note to 'Geometric Extent' of Warning Area: APS is based on a one-dimensional, logical representation of the railway network => track axis. In order to be able to process any form of geometrical and/or geographical algorithms that are able to identify a surface area (e.g. geometric extent on track axis times lateral extent). Future warning systems must be able to add a geometric and/or geographic area with a lateral extent of an APS Warning Area.*

4.4.3.1 Proposed representation of a Warning Area

The geometric representation of a Warning Area in operating state is practically identical to a Usage Restriction Area, therefore it is not being shown here. But a Warning Area will have different/additional attributes to enable for instance:

- A representation of its general state (i.e. active, inactive) as selected from the actor responsible for safety within the working area, called 'field responsible person' hereafter
- A representation of its warning state as demanded from APS (e.g. warning demand acknowledged)
- A representation of the Warning System considering one or multiple addressed Warning Device/s as configured by the actor 'field responsible person' and used from APS to send Warning Commands to and receive acknowledgments or rejects from interconnected Warning Devices
- Referencing one or multiple existing Usage Restriction Area/s as configured by the actor 'field responsible person' for instance, if needed in addition
- Carry a unique identification of the actor 'field responsible person' in charge of this Warning Area in order to activate, inactivate or delete warning areas

4.4.3.2 Proposed general working principle

Warning Areas are (typically) planned and configured in the course of track work maintenance planning and Warning Systems are installed on-site prior to their required use.

Note: The general working principle has not yet been agreed upon and will be added in the next release. The next sections of this chapter cover basic functionalities to be implemented in the general working principle and refer to the Warning Area concept presented so far.

4.4.4 Migration

As with the rest of the proposed concept, APS can be implemented without the need to utilise Warning Areas, e.g. when on-site warning signals releases are secured by human beings or alternative technical solutions. APS does however allow an interaction with Warning Systems from the very beginning if required from an IM.

From IM's perspective, the choice of using this functionality is completely open and independent of the introduction of APS.

4.4.5 Degraded modes

Nr.	Scenario	Details	Consequences	Mitigation action/s by APS
1	Warning Command rejected	• APS sends a Warning Command prior to being able to grant a Movement Request partially or fully covering the geometric extent of the corresponding Warning Area • This Warning Command is being rejected by the Warning System	• MP (update) cannot be granted • Train unit movement comes to an unplanned standstill	• Process outside of the scope of APS • MP request reinitiated from PE with lower maximum speed (depending on configured safety condition) • *Note: Fallback with APS user interface possible when PE is not available*

2	Warning Command not acknowledged (nor rejected)	As with #1	As with #1	As with #1
3	Warning not released onsite despite acknowledgement	Despite that the Warning System has acknowledged the Warning Command from APS, the Warning System does not issue a Warning on-site prior to the approaching train unit	Track Worker within Warning Area in potential risk of being hit by approaching train	To be analysed when doing hazard analysis: Feeding back the event of a Warning release from Warning System to APS as criteria for e.g. emergency break would trigger when communication between Warning System and APS is not working
4	Train unit moves (far) slower than requested	• The requested speed profile in the MP was the basis for the calculation of the absolute/relative time when a Warning has to be issued by the Warning system • The Warning would be released before the agreed lead time	• Track Workers might be tempted to access the track area after N Seconds/Minutes and therefore Track Worker within Warning Area is in potential risk of being hit by the delayed approaching train • Safety condition violation identified by APS	To be defined: APS may send a further Warning Command that allows the Warning System to either release the Warning at a later point in time or to release another Warning signal indicating an earlier / a delayed entry of the approaching train unit

4.4.6 Delta

A major difference in between today's system environment can be seen in the standardisation of the interfaces between APS and Warning Systems without the need to reconfigure generic safety conditions or to execute a safety assurance when interconnecting Warning Systems with APS.

The proposed use of a Warning Area supports the objectives towards higher track worker safety for instance with the possibility to perform two-face commits (the person in the field to be protected confirms the removal of a Warning Area) and a validation of the location (reduce the risk of removing a wrong Warning Area).

4.5 Managing Transitions

4.5.1 Objectives and System Requirements

Objective	System Requirements
APS@Support the transition of a train movement between a legacy interlocking/RBC and an APS Area of Control in both directions without limiting operation	$APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to an adjacent APS Area of Control without manual interaction $APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to adjacent legacy signalling system without manual interaction $APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to adjacent track section, not equipped with any signalling system $APS shall ensure that the transition of a train unit movement between two Area of Controls does not require stopping the train unit
APS@Support safe handovers of movements from and to adjacent legacy safety systems	

Objective	System Requirements
	$APS shall ensure that the transition of a train unit movement between two Area of Controls does not reduce the operationally required maximum speed of the train unit
APS@Support lineside signals at Area of Control transitions to and from legacy interlocking/RBC systems	$APS shall support transitions from and to neighbouring areas equipped with lineside signals located at the border either in the own AoC or in the neighbouring area

4.5.2 Problem description

Typically, two neighbouring interlocking systems are separated from each other with block signals or border signals symbolising the exact border or responsibility of the different systems and/or operators.

Depending on the type of construction (e.g. automatic, central block signal), there are more or less controlling interactions possible for the signaller in charge. Commonly to each block design are the interfaces to its neighbouring signalling system (e.g. interlocking system). It is checked whether the adjacent main signal shows stop and its substitute signal is extinguished before a signal can show proceed. There is/are no European-wide standardised interface/s defined between interlocking and block (signal) systems. However, national solutions do exist. Next to interfacing interlocking systems, different solutions exist for train number reporting systems to allow train location tracking for operational purposes.

The different European railways and suppliers have deployed a variety of different solutions to interface adjacent interlocking and train number reporting systems over decades. Standardising interfaces for a future signalling systems environment shall consider a couple of different migration scenarios to which the standardised interface can be adapted to.

At the boundaries of the Area of Control of an APS, transitions to other neighbouring interlocking will be required in order to allow a safe entry into an Area of Control of APS and vice versa. Therefore, APS will have to communicate with neighbouring signalling systems. A neighbouring signalling system could be another APS or a legacy interlocking or a block system. A signalling system environment of an IM will most likely be divided into several geographic sectors. Therefore, transitions between APS and neighbouring APS, to legacy interlocking and block systems must be made possible. In addition, different ETCS level/modes between these borders have to be supported. The ETCS level describes the fit of function of the line and at a border, different functions may be used.

A future standardised interface must at least cover these two main functionalities:

- Securing a route path (a Movement Permission) between an APS and a neighbouring APS or legacy signalling system or connected track segment without any specific signalling system with entry/exit to APS
- Handing over a moving train from one APS to the neighbouring Train Control system e.g. equipped with a Radio Block Centre (RBC) and vice versa

In legacy application two adjacent trackside systems (e.g. RBCs) communicate over a defined interface. The functional principle and interface of this handover is described in the TSI CCS. Route related topology information will be exchanged. APS has to ensure the interplay with a RBC in the neighbouring signalling system.

4.5.3 Solution approach

At this point in time (December 2021), there is a detailed concept and solution approach available from the Swiss Federal Railways (SBB) which is not yet discussed or agreed upon on an international level. The assumptions, preconditions and identified main requirements made for this SBB detail concept are being listed below and shall be regarded as discussion basis.

- APS Movement Authority Transactor supports the ETCS Handover protocol and procedure defined in SUBSET-026, SUBSET-039 and SUBSET-098.

- An APS transition will be usually implemented on an open line (mainline track section).
- One APS shall exclusively use Map Data of its own Area of Control but not require detailed Map Data of the topology of neighbouring systems. Map Data shall only provide the minimum set of information from the neighbouring Area of Control in order to allow a safe entry and exit into and from the own Area of Control. This allows the highest possible independency while processing engineering data from the side of Map Data.
- Movements to border or near to border of Areas of Control and back again without a transition over border should be supported including safety validation of risk buffer by neighbouring APS in case the risk buffer reaches into the neighbouring APS.
- Two train unit movements that are following each other across APS borders at a minimum possible distance (maximum capacity) should be supported including safety validation of the risk buffer.
- APS instance does not need to have any topology information of the neighbouring APS for the calculation and safety validation of the risk buffer reaching into neighbouring system.
- Neighbouring APS could be from different suppliers with different algorithm for the risk buffer calculation

Based on this concept, some overall aspects are currently derived within the first concepts of APS handover:

- The handover between two APS Area of Control or an APS Area of Control and a legacy signalling system, equipped with an RBC shall be handled in the Device Abstraction Layer.
- The Movement Authority in the handing-over APS is enlarged by the received Movement Authority of the accepting APS, based on the Movement Permission granted in the accepting APS.
- Additional information exchange on Safety Layer is needed only for some information concerning track clearance.

The operational handover must be performed on operational level, including the in-time request of the several Movement Permissions in the different Areas of Control.

4.5.4 Migration

The previously mentioned detailed concept for managing transitions drafted by SBB also includes a proposal for a migration strategy. The migration concept is based on using existing TMN blocks because they form most of the interfacing technologies deployed in Switzerland.

APS must consider a generic migration approach to be mapped to the several existing systems in the field by the different Infrastructure Managers.

4.5.5 Degraded mode

As today, there will be situations that need to be resolved by the systems involved or manual processes or combinations of them. Examples:

- Neighbouring system does not release block section despite of being cleared of train unit
- Neighbouring system requests blocks section with invalid or incomplete information in its request
- Train unit comes to an unplanned halt within two neighbouring systems
- Handover with ETCS information exchange fails

4.5.6 Delta

Applying a standardised interface between an APS and a legacy signalling system and between two adjacent APS systems will allow:

- A reduction in integration efforts
- A reduction of LCC dependency between the systems/components involved
- A harmonisation of operational rules, processes and its consequences for all operating staff involved (signaller, dispatcher, train driver)
- Set a basis for GoA2 and upwards in order to reduce complexity of for instance functionalities required to transfer a GoA2…GoA4 movement from one Area of Control to another – particularly also when crossing IM borders.

4.6 Managing Configurations

4.6.1 Objectives and System Requirements

Objectives	System Requirements
APS@Enable individual adaptation of the basic configuration without having to adapt the safety case and the functionality of a component for it	$The definition and configuration of safety conditions to be checked by APS shall not contain site or location specific references $APS must support the configuration of safety conditions according to an IM's needs
APS@Provide a set of safety functions with a basic configuration that enables safe railway operation	$APS shall provide a default configuration that allows safe movements on any railway network topology that complies with the defined application conditions $Default configuration shall contain values which can be changed within an unambiguously defined range to adapt to an IM's requirements $APS must ensure that erroneous configuration data changing a default configuration does not disable the corresponding safety check
APS@Support exchange of hardware and software components with the same functionality treated as 1:1 maintenance with less need of system approval	$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) during any installation procedure $All APS interfaces should be specified in an unambiguous, exact and testable way $APS subsystem software approval must be possible independent of configuration data $APS hardware and software approval must allow 1:1 exchange as maintenance activities within the authorisation for placing on the market or placing in service
APS@There shall be no need to restart SubSys APS when interfaced component versions change	$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) during any installation procedure $Identification of an incompatible version/built (transport, marshalling, application model) shall be revealed (e.g. towards Monitoring) and must not violate the RAMS and the non-functional requirements $APS shall support the exchanging of interfaced subsystems/ component during runtime without affecting the RAMS conditions of APS and without a need to restart any other subsystem/component $APS shall be developed in such a way that it can be used independently of the life cycle of the runtime environment
APS@Allow flexible adaption to data volumes and frequencies without the need to change the code basis	$Build a system that is capable of handling the highest RAMS and non-functional Requirements of an IM $APS shall support the deployment of a scalable system $APS shall enable by configuration to consider different data volumes processed in a certain time and use different frequencies e.g. for demand of update of cyclic data without a need of change on the code/algorithm
APS@Allow flexible adaption to data volumes and frequencies without violating the RAMSS specifications	$Define formal values / value ranges for each RAMS and non-functional requirement in combination with the corresponding runtime environment (e.g. hardware, operating system) $Build an APS that can handle the highest RAMS and non-functional requirements as a sum of all agreed needs of different IM

Objectives	System Requirements
	$APS shall enable by configuration to consider different data volumes processed in a certain time and use different frequencies e.g. for demand of update of cyclic data within the limits of the RAMSS specification of the default configuration
APS@Incompatibility between an interconnected field element must not violate the SubSys' RAMSS requirements	$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) in the course of any installation procedure $Identification of an incompatible version/built (transport, marshalling, application model) shall be revealed (e.g towards Monitoring) and must not violate the RAMS and the non-functional requirements $APS shall support exchanging subsystem software versions during runtime without affecting the RAMS condition of APS and without a need to restart any other subsystem/component
APS@Support the change of a SubSys' software version during runtime without affecting the RAMS specification	
APS@Event patterns for the identification of safety rule violations shall be configurable including the required safety measure	$APS must support the configuration of safety conditions according to an IM's needs $APS safety reactions shall be unambiguously specified $APS shall provide a set of safety reactions, the IM can choose for implementation for handling of specific situations on the needs of the IM based on the specific safety case of the trackside system integrated by the IM $APS shall support the configuration of values within value ranges for specific safety reactions for each identified safety violation
APS@Support the configuration of national specific operating rules	$APS shall consider customisable system parameters following national rules and laws, e.g. speed allowed in certain situations $APS must enable or disable distinctive functions if they are not allowed to be used by national operational rules by keeping other distinctive core function present
APS@Support the segmentation of Map data in order to define Areas of Control of an APS	$APS shall expect that each Map Data delivery encompasses the entire fail-safe track network topology according to the application conditions of the entire Area of Control $APS shall expect that each concerning Edge terminates at a dedicated Node at the spot location of an Area of Control border $APS shall expect a Map Data delivery as a list of new, changed and deleted topology objects in order to support updating its operating state $APS shall support the unambiguously specified Map Data and its semantics $APS shall expect that each Map Data delivery that differs from a previous delivery has a unique identifier in order to distinguish an update from a redelivery $APS shall expect that each Map Data delivery is received unchanged from the source

4.6.2 Problem description

As already addressed in chapter 2.1.1, the required project engineering data for today's legacy CCS environments is typically managed with proprietary engineering tools (IM specific, supplier specific), accompanied by a high number of manually supported process and validation steps. Additionally, legacy interlocking systems

support a multitude of functions as addressed in chapter 4.3.5, adding an additional degree of complexity to the overall project engineering.

4.6.3 Solution approach

By applying the proposed core principles, solution approaches and the discontinuation of trackside element installations, the overall complexity of the project engineering effort required can be significantly reduced. Of course, there will still be project engineering efforts required for planning and designing new or changed track sections. The engineering efforts contain hardware engineering and configuration including communication hardware and encryption devices for interfacing e.g. new large areas to be added to the system but to be split from an architectural view.

The generic and unified representation of the railway network topology (part of Map Data) will comprise fewer objects; applying a generic safety logic will allow to produce safe train unit movements, regardless of the underlying Map Data. Operationally driven functionalities shall consequently be realised outside of the APS' system borders, allowing a higher pace of development and release cycles on the side of PE/TMS.

APS shall be realised with a minimum set of safety conditions and safety reactions that will be configurable in order to adapt to an IM's requirements. The configuration of APS encompasses for instance the definition of:

- A value from a (unambiguously specified) value range. Examples may be the configuration of
  - the speed limit over which flank protection method on a high level e.g. by points is required
  - the maximum speed limit over which a Risk Buffer is required
- Values, value ranges from adjacent railway networks where transitions from and to an APS Area of Control is required. Examples may be
  - the maximal allowed entrance speed, e.g. based on the signalling and train control principles of the adjacent system
  - the specific exit speed condition, e.g. based on the block section length in the adjacent system
- Predefined safety reactions, defining which safety reaction shall be processed if a violation of a certain safety condition has been identified
- Values handling the suitability of all authorised onboard units per specific region, e.g. by known of unique ETCS-ID or stored keys for communication

It is proposed that when defining safety conditions, safety violation definitions and safety reactions, each definition shall be unambiguously specified together with all values that shall be configurable plus the resulting consequence in the processing logic in form of unambiguously specified (binary) outputs, if possible.

4.6.4 Migration

As stated in chapter 2, some prerequisites are mandatory before deploying an APS, such as for instance the availability of a fail-safe topology data representation and the existence of Object Controllers.

From a configuration point of view, collecting, validating and representing railway network topology data long before APS shall be deployed may be beneficial to an IM at a very early stage, being able to utilise such data already with/for systems already in use (e.g. starting automated project engineering processes, starting to deploy Object Controllers) or which will be used independently from APS (e.g. a Traffic Management System). This forms a generic and standardised railway network topology representation.

At a later stage, generic representation of additional objects (e.g. Allocation Sections, additional usage conditions such as loading gauges) may be added in order to be used either in connection with an APS or with existing applications. Validation of Map Data in order to become fail-safe may be a process that could be established over a longer period of time and even in conjunction with existing project engineering.

Migration to an APS may be most cost effective when replacing multiple legacy interlockings with APS at a time in order to reduce integration efforts to and from adjacent interlockings/block sections. Also, when considering the (eventual/most likely) change towards line side signalling to cab signalling, a larger stretch of track network may be the most feasible solution for an IM, for reducing a small-stepwise ongoing migration needs efforts for many adaptions, operational and approval processes.

4.6.5 Degraded Mode

There will be not much of a degraded mode when it comes to configuration; either a configuration is available or not. If no configuration is available to APS, APS won't be able to perform any Request checks.

The way APS stores and initialises its configuration(s) will need particular attention in order to fulfil all RAMS and non-functional requirements.

Thus, all potential situations must be detailed in system design for definition of the behaviour. This must include unlikely situations too. It can be defined, if APS will perform in some situations in case of changes in configuration background functions, but no functions enabling operation.

4.6.6 Delta

The main differences between today's legacy CCS environments and APS regarding configuration(s) will be:

- Very little configuration effort required on the side of APS due to generic rule sets and generic representation of the railway network topology and its trackside elements plus the generic representation of any form of occupancy claim through object aggregation.
- Some configuration efforts are still required so that APS becomes functional such as for instance:
    - Map Data but due to the omission of a large number of trackside elements such as light signals and with them preconfigured route paths, predefined dependencies for flank protection and so on; the configuration efforts will be reduced significantly
    - Object Controller must be correctly configured for the APS needs and the defined interfaces, while the Object Controllers need to translate electrical signals from/to switchable field elements and further trackside elements into e.g. EULYNX commands and vice versa, plus submit characteristics of the trackside elements they interact with
    - Transactors will require a certain amount of configuration effort in order to adapt to the technology deployed
    - Network communication will also need a configuration (routing, security, authentication and authorisation integration, etc.)

5 Conclusion and Next Steps

This document is the first draft of an APS concept. It contains system requirements for APS derived from the current first proposals of business targets and business objectives. These will need to be agreed upon at a later stage of the program.

The presented detailing of fields of consideration within the previous chapters shall be detailed in specific Detailed Concept Papers.

Next steps with potential impact on this documentation and the overall development of APS may be:

- Alignment and definition of the Business Targets, Objectives and System Requirements on European level to derive the impact on priorities for detailing the functional scope of APS.
- Consideration of eventual migration strategies (influences the scope of APS in the field of e.g. interfaces and transitions, degraded modes and derived functional requirements, alignment and integration with ATO strategy/strategies)
- Alignment and definition of generic non-functional requirements on European level (e.g. Maximum number of supported field elements per APS Area of Control, quantities and frequencies of localisation information messages received and processed, max. processing times, etc.)
- Alignment of functionalities to the requirements of the subsystems linked with APS and their corresponding interfaces

Annex A: List of objectives

Table 1: A.P.M. objectives relevant for APS

Objective	Category
APS@Handle failures and degraded modes of other RCA SubSys efficiently	Automation
APS@Handle internal failures and degraded modes efficiently	
APS@Minimize the transfer of one or many safety responsibilities to a human operator even in degraded situations	
APS@Support interfacing to additional field elements during runtime	
APS@Support published changes in Map Data (new, change, delete) during runtime without impact on operation	
APS@Ensure the generation of a fail-safe operating state after a reboot	
APS@Update of safety demonstration documentation after replacement automatically	
APS@Use interfaces with automatic adaptions and internal intelligence for interfacing different versions of building blocks without the need of upgrade existing building blocks based on change in interface	
APS@Disclose incompatibilities between building blocks and SubSys and their interfaces (i.e. incompatible software versions, incompatible protocol versions)	
APS@Ensure the generation of a fail-safe operating state after a reboot	
APS@Apply a generic safety approach in encapsulating smallest possible safety relevant functions in building blocks that allow a separate safety approval	Functional independency
APS@Demonstrate safety within the building blocks including its interface without knowledge or need of assumptions on the function of further building blocks behind the interface	
APS@Encapsulate minimal viable functionalities in building blocks to enable an individual configuration of the building blocks and simple interfaces	
APS@Ensure process and system independence (control safe usage of track section regardless of how the rail network topology is physically realised)	
APS@Separate railway network topology data from functional code	
APS@Support independent updateability of Hardware, Software and Engineering Data	
APS@Separate trackside assets from interlocking software	
APS@Allow the replacement of components without changing the system safety case	Generic product assurance
APS@Enable a safe system and its safety assurance based on building blocks in order to minimise effort for safety assurance	
APS@Ensure safeguarding of movements for any railway network topology that is compliant to the safety-related application conditions	
APS@Minimise effort for safety assessment	
APS@Perform generic hazard management by an overall system authority	
APS@Consider hazards of current solutions and reduce impact through system design	
APS@Delegate non-safety relevant functions to planning system	
APS@Reduce need of Infrastructure Manager related hazard evaluation	
APS@Support exchange of hardware and software components with the same functionality with less need of system approval	
APS@Enable implementation of APS on existing track layout without changing it	Independency from project planning
APS@Separate the safety logic system from operational planning systems	
APS@Use the same high parameterisable safety level for any railway network topology (includes safe control at any time of existing and interfaced trackside assets)	

APS@Provide a uniform user operating concept, independent of the site-specific rail network	
APS@Allow the replacement of multiple legacy interlocking with one single APS	Life cycle costs
APS@Enable cab-signalling for all movements	
APS@Enable changes, adaptations and extensions throughout the life cycle of the building blocks	
APS@enabling predictive maintenance by data capture for increasement of overall availability	
APS@support the TSI CCS enhancements (e.g. “always connected” UNISIG-CR 1350, “cab anywhere” UNISIG-CR 1367)	
APS@usage of different train localisation technologies for reduction of costs for trackside train detection system	
APS@Use standard interface towards Field Elements to separate the lifecycles of hardware and software components	
APS@Capturing of operational data covering RAMSS performance requirements and assumptions during operation	
APS@Enable individual adaptation of the basic configuration without having to adapt the safety case and the functionality of a component for it	Managing configurations
APS@Provide a set of safety functions with a basic configuration that enables safe railway operation	
APS@Support exchange of hardware and software components with the same functionality treated as 1:1 maintenance with less need of system approval	
APS@There shall be no need to restart SubSys APS when interfaced component versions change	
APS@Allow flexible adaption to data volumes and frequencies without the need to change the code basis	
APS@Allow flexible adaption to data volumes and frequencies without violating the RAMSS specifications	
APS@Incompatibility between an interconnected field element must not violate the SubSys’ RAMSS requirements	
APS@Support the change of a SubSys’ software version during runtime without affecting the RAMS specification	
APS@Event patterns for the identification of safety rule violations shall be configurable including the required safety measure	
APS@Support the configuration of national specific operating rules	
APS@Support the segmentation of Map data in order to define Areas of Control of an APS	
APS@Support lineside signals at Area of Control transitions to and from legacy interlocking/RBC systems	Managing Transitions
APS@Support safe handovers of movements from and to adjacent legacy safety systems	
APS@Support the transition of a train movement between a legacy interlocking/RBC and an APS Area of Control in both directions without limiting operation	
APS@Interface with mobile devices in order to confirm the removal of a usage restriction area	Occupancy claims NOT identifiable with localisation technology
APS@Interface with mobile devices in order to safely represent the existence of a usage restriction area	

APS@Only current occupancy claims and usage restrictions that forbid any movements shall hinder a movement	
APS@Enable automatic warnings areas and movement limitations without the need for manual interactions	Managing Warning Areas
APS@Prevent granting a movement over predefined geometrical areas without prior warnings to track workers	
APS@Provide functionality to define geometrical extents for warning areas within the Area of Control	
APS@Support interfacing with existing warning systems for track workers	
APS@Support safe entry and exit from a construction site or maintenance location for track worker and machinery	
APS@Allow safe movements also when train characteristic are unknown	Safety checks
APS@Allow still safe best production under circumstance of reduced availability of reliable information	
APS@Build a system that doesn't consider in its logic operational implications but only checks for safe operation (separate business logic and safety logic)	
APS@Consider speed limitations only on the specific geometric extent	
APS@Consider train specific characteristics when granting movements	
APS@Grant movements considering the operational needed safety level and the possible risk mitigation measures	
APS@Guarantee safeguarding of all movements on railway tracks within a geographical region	
APS@Identify safety rule violations during runtime and initiate safety measures in order to mitigate safety hazards	
APS@Implement a strict object aggregation for enabling of usage of different information sources and simplification of interfaces within the system and future adjacent systems (avoid the need to implement a logic knowing exact behaviour of interfacing parts)	
APS@Implement full supervision of all movements, also shunting	
APS@Presuppose the existence of a radio-based Train Control System (ETCS) assuming a continuous communication connection to each train on-board unit	
APS@Provide measures to reduce hazard when safety rule violation is identified	
APS@Provide real-time operating state	
APS@Regard Map data as fail safe	
APS@Support FRMCS for communication between track side and onboard	
APS@Provide operating state towards mobile devices	
APS@Publish safety rules and config data towards operational level	
APS@support automated coupling	
APS@support connectionless communication also via FRMCS	
APS@Support different ATO levels (GoA1 – GoA4)	
APS@Consider open interfaces to integrate as much formats as possible	Standardised interfaces
APS@Develop and commission standard interfaces	
APS@Enable usage of mix of different ETCS OBU system versions on line (migration facilitation)	
APS@Ensure functionality even in case of incomplete information due to limited functionality of interfaced components	

APS@Ensure interface compatibility to legacy interlocking systems still equipped with line-side signalling	
APS@Separate data aggregation from data provisioning	
APS@Support EULYNX standards for interfacing with field elements via Object Controller	
APS@Use of existing infrastructure without the need of changes/alignment due to the use of APS	
APS@The building blocks and their interfaces should have as little version dependency as possible	
APS@Introduce generic capabilitiy-based interfaces	
APS@Support the AoC segment size of the interfaced Plan Exection	
APS@Allow the replacement of different trackside devices implementations that comply to the standardised (transactor) interfaces with other implementations without effort	
APS@Ensure network wide adaptability towards changes of the trackside CCS SubSys	
APS@Consider continuous precise onboard localisation information (speed/extent)	Occupancy claims identifiable with localisation technology
APS@Enable usage of train integrity information for optimised track occupancy without the restriction of fixed signalling blocks	
APS@Ensure integration of new localisation technologies that will only emerge in next future years	
APS@Guarantee railway operation with a mixed ETCS level approach (L2/HL3/L3) of trains and rail network	
APS@Provide Ability for safe train movement on arbitrary railway network topologies with at least one clear-track signalling or localisation technology installed	
APS@reduction of CCS trackside equipment on a needed level for operation by gaining capacity not only with standard CCS trackside enhancements (e.g. trackside train detection sections, shorter routes)	
APS@Support continuous and uninterrupted localisation of train units (“always on”)	
APS@Support different localisation systems and localisation technologies for trackbound and non-trackbound objects in order to represent safely non-occupied track segments	
APS@Support future train integrity and safe length information from the very beginning	
APS@support only of ETCS Level 2 and 3 (also mixed on the same line)	
APS@Support the aggregation of multiple localisation information in order to represent the entire occupancy claim of train units	
APS@Support the securing of route paths with any geometric extension with no need having a fixed start and end point defined by lineside signals	
APS@Clear secured route path immediately when clearance has been identified (i.e. using safe train length, localisation tag) in order to maximise track capacity	
APS@Enable usage of train length and integrity information for optimised track occupancy without the restriction of fixed signalling blocks and/or train detection sections	

Annex B: List of the derived requirements

$Any functionality not declared safety-relevant shall be realised out of scope from APS

$APS shall be considered in the safety management process of RCA and be compliant with the safety requirements identified during the risk analysis

$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block

$The combined use of functional building blocks shall not require an additional safety assurance

$All APS interfaces shall be defined with unambiguous semantics

$All APS interfaces should be specified in an unambiguous, exact and testable way

$The behaviour of the individual APS components shall be unambiguously specified

$APS shall consider the provided Map Data as fail safe

$APS functions shall be failsafe executable using any Map Data provided if the data complies to the application conditions

$APS shall ensure that the application code only works on abstract representation of the topology

$All APS interfaces should be specified in an unambiguous, exact and testable way

$APS must ensure Engineering Data independent approval

$APS must ensure Software-independent approval

$APS must ensure Hardware-independent approval

$Ensure clear layering for transport, marshalling and application model

$APS shall ensure that the application code only works on abstract representation of the topology

$The behaviour of the individual APS components should be for-mally specified when required by formal validation

$All APS specifications shall be freely available to anybody at no cost

$All partners shall sign an open-source agreement at the very beginning of the project

$All contributions to APS specifications fall under the agreed open-source agreement

$No participant may claim any rights to the APS specifications or further work results openly published under the agreed open-source licence

$APS shall provide information on its interfaces in such a granularity and format that it is suitable for target systems to consume the information correctly and efficiently

$APS shall be able to process information of varying quality on its interfaces

$APS shall support the safe movement of a train unit from an APS Area of Control to an adjacent legacy signalling system and vice versa

$The speed of a train movement shall not be limited due to the transition between an APS Area of Control to an adjacent legacy signalling system itself but only due to any rail network speed restrictions

$APS shall process localisation information from existing TTD systems

$APS shall not rely on the existence of localisation information from existing TTD systems to identify track occupancies

$APS shall consider all safety relevant railway network usage conditions prior to safely granting a movement for a train unit

$APS shall provide interfaces that are compliant to the TSI CCS

$APS shall provide interfaces that are compliant to EULYNX interface specifications

$APS shall not require an adaptation of the infrastructure when put into operation

$All APS interfaces must provide multi version support

$APS shall provide interfaces that are compliant to the TSI CCS

$APS support different ETCS system versions within the same APS Area of Control

$APS shall support different localisation technologies that may deploy different reference systems with different data formats on their interfaces

$APS shall process localisation information from a variety of localisation systems and technologies

$APS shall use a unified and generic representation of identified track occupancies, independent of the localisation technologies used

$APS shall ensure that the application code only works on abstract representation of the topology

$APS shall support the segmentation of MAP data from interfacing systems

$APS building blocks shall work independently of the functionality of neighbouring blocks, therefore no assumptions about dedicated behaviour shall be made

$APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations

$Ensure safety relevance of each component to prevent components from suddenly becoming safety relevant in a later implementation

$APS functions must be failsafe executable using any Map Data provided if the data complies to the application conditions

$APS must ensure Hardware-independent approval

$Safety checks shall be independent of operational procedures

$The integration of building blocks with their own safety assurance shall result in a safe system that does not require further safety approvals.

$The combined use of functional building blocks shall not require an additional safety assurance.

$APS shall be compliant with the safety requirements identified during the risk analysis

$The safety processes of the APS solution design (supplier activities) and the APS concept design (IM activities) shall be aligned

$APS shall be compliant with the safety requirements identified during the risk analysis

$APS shall be developed using a robust software development process according to CENELEC standards

$Safety checks shall be independent of operational procedures

$APS risks shall be limited to safety-relevant aspects without considering business-critical risks to the railway performance

$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block.

$The definition and configuration of safety conditions to be checked by APS shall not contain site or location specific references

$APS shall provide identical functionalities for any kind of operational movements

$APS shall provide a default configuration that allows safe movements on any railway network topology that complies with the defined application conditions

$APS shall support the safe movement train units on an arbitrary railway network without major adaptations of existing trackside assets

$Within the Area of Control, APS shall support minimally 1250 switchable field elements

$Within the Area of Control, APS shall support minimally 3.000 TTD

$Within the Area of Control, APS shall support the safe production of minimum of 75 simultaneous train units (moving, stopped) per hour

$APS shall be interfaceable to a various number of present Object Controller in compliance to the EULYNX standards, interfaced to different legacy interlocking systems

$Ensure an agreed and committed life cycle policy between all suppliers for investment protection

$Future sematic changes shall under no circumstance require changes in the interfaces

$APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)

$Provisioning of measurement data must not influence the performance of APS

$APS shall provide quantities and frequencies of processed data towards Monitoring

$Provisioning of measurement data shall not influence the performance of APS

$APS shall not rely on the existence of localisation information from existing TTD systems to identify track occupancies

$APS shall disclose and support the handling of failures from interfaced RCA SubSys

$APS shall disclose and support the handling of internal failures

$APS shall support and provide guidance for manual operation on a fallback user interface

$APS shall support the transfer of Safety Responsibility in an automatic way

$APS shall consume MAP data updates during runtime

$APS documentation shall be generated automatically and stored in an efficient document management system

$APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)

$APS shall support the automatic identification and recognition of different system configurations and versions during runtime

$APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime

$APS shall recover efficiently after a reboot

$APS shall continuously provide and monitor the current operating state including during the initialisation phase, re-boot and after changing interfacing (sub-)systems

$APS shall process on-board localisation information for aggregation of the track occupancy

$APS shall support continuous localisation information to represent track occupancy

$APS shall use train integrity information provided by on-board or trackside for aggregation of the track occupancy

$APS shall enable track occupancy independently from fixed signalling blocks definition

$APS shall release each section of a secured route path after safely identifying its clearance based on train integrity information calculated safe rear end

$APS shall use on-board localisation information for aggregation of the track occupancy

$APS shall be able for interfacing new localisation technologies

$APS shall represent any track occupancy as generic representation to be as independent as possible from formats of localisation devices

$APS shall operate on different lines equipped with different ETCS level starting from Level 2

$APS shall support different ETCS levels simultaneously

$APS shall base the granting or rejecting of requested movements on track occupancy claims and field element states

$APS must consider all usage restriction conditions of the track segments claimed for a movement

$APS must represent any track occupancy in a fail-safe way

$APS must represent any usage restriction in a fail-safe way

$APS shall be Safety Responsible for fail-safe granting movements to train units

$APS shall be able to identify track occupancy with at least one trackside train detection system or localisation technology installed in the Area of Control

$To represent track occupancy, APS shall be able to use a mix of trackside train detection system and localisation technologies installed in the Area of Control

$APS shall support the aggregation of track occupancies along tracks not continuously equipped with trackside train detection system in conjunction with other localisation technologies

$APS shall enable operation without the need of installed contiguous trackside train detection system

$APS shall enable operation without the need of lineside signalling system

$APS shall not limit the start and end of movements to specific positions in the Area of Control

$APS shall process mobile localisation device information of trackbound objects for aggregation of the track occupancy

$APS shall process mobile localisation device information of non-trackbound objects for aggregation of track occupancy

$APS shall be able to represent track occupancy using safe train length information

$APS shall release each section of a secured route path after safely identifying its clearance based on train integrity information

$APS shall support different ETCS levels simultaneously

$APS shall only support ETCS levels equal to or higher than L2

$APS shall support the aggregation of track occupancies along tracks not continuously equipped with trackside train detection system in conjunction with other localisation technologies

$APS shall release a section of a secured route path after safely identifying its clearance based on train integrity information

$APS shall consider safe train length information and integrity state for object aggregation for efficient track occupancy

$APS must support the confirmation of a URA removal from a mobile device

$APS must ensure that URAs with safety relevance are not removed without adequate confirmation

$APS must represent the operating state towards mobile devices in a fail-safe way

$APS must represent any Map data in operating state in a fail-safe way

$APS must represent any usage restriction in operating state in a fail-safe way

$APS shall not prevent a movement of a train unit with unknown characteristics

$APS must comply to defined safety conditions

$APS shall allow movements under specific conditions, when localisation information becomes unavailable

$APS shall allow movements under specific conditions, when states of switchable field elements become unavailable

$APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back

$APS must not grant a movement when safety conditions are violated

$APS must be able to identify safety condition violations

$APS must take one or multiple safety measures when a safety condition violation is identified

$APS must support the configuration of safety conditions according to an IM's needs

$APS shall support the transfer of Safety Responsibility in an automatic way

$APS shall not consider any operational consequence when granting movements but solely if the movement is safe

$APS shall prevent a train movement from exceeding a speed limitation within its defined geometric extent

$APS shall prevent movements when safely known train characteristics violate usage restrictions defined in the usage restrictions of the track section claimed for this movement

$An IM shall have the possibility to configure safety conditions according to its requirements and regulations

$APS shall consider the safety conditions configured by an IM according to its requirements and regulations

$APS shall not prevent a movement of a train unit with unknown characteristics

$APS shall allow movements under specific conditions, when states of switchable field elements become unavailable

$APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back

$APS shall allow the geometric overlap two route paths complying to the defined safety conditions

$Each safety condition APS check shall be unambiguously specified

$Each safety condition violation, identified by APS, shall be unambiguously specified

$Each safety measure, APS and its resulting safety condition cause, shall be unambiguously specified

$An IM shall have the possibility to configure parameters for each safety condition, each safety condition violation and each safety measure according to its requirements and regulations

$APS shall consider parameters for each safety condition, each safety condition violation and each safety measure configured by an IM according to its requirements and regulations

$All APS interfaces must be defined with unambiguous semantics

$All APS interfaces should be specified in an unambiguous, exact and testable way

$APS shall encapsulate translation logic from processing logic

$APS shall implement a strict object aggregation, based on abstract concepts

$APS shall not prevent a movement of a train unit with unknown characteristics

$APS shall implement full supervision of shunting movements

$APS shall provide interfaces that are compliant to the TSI CCS

$APS shall consider to handle trains with continuous communication connection

$APS must prevent collisions

$APS must prevent derailments

$APS must represent any track occupancy in a fail-safe way

$APS must represent in real-time all movable objects within its AoC in a fail-safe way

$APS must represent in real-time all granted movements in a fail-safe way

$APS must represent in real-time the current state of a switchable field element in a fail -safe way

$APS shall support GSM-R for a transition period

$APS shall support FRMCS technology based communication technology for all communication purposes between onboard and trackside

$APS must represent in real-time the current state of a switchable field element in a fail-safe way

$APS shall make the generic safety rules and the specific configuration data of the function make available for the operational level

$An IM shall have the possibility to configure parameters for each safety condition, each safety condition violation and each safety measure according to its requirements and regulations

$APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back

$APS must consider Warning Areas when granting movements

$APS must communicate with Warning Systems in order to send warnings and to receive acknowledgements

$APS must make sure that prior to any movement within a Warning Area, an onsite warning – according to defined conditions - will be issued

$Before granting a movement, APS must secure that the configured minimum pre-warning time is not violated

$Before granting a movement, APS must secure that the configured maximum pre-warning time is not violated

$An IM shall have the possibility to configure the minimum and maximum pre-warning time

$APS must ensure that the Warning System has confirmed the Warning Command by APS before granting a movement

$APS must be able to update a previously issued Warning Command

$APS shall provide a functionality to create, change and delete geometric extents in operating state, representing a Warning Area

$APS shall support the creation, change and deletion of a Warning Area to the authorised actors Plan Execution and human beings

$APS must prevent that Warning Areas geometrically overlap

$APS must support the transmission of a Warning Command to a Warning System in the field

$APS must support the reception of a Warning Command acknowledgement from the Warning System

$APS must issue an individual Warning Command for each individual train unit

$APS must be able to issue Warning Commands in case of an identified runaway vehicle that may enter a working area

$APS must be able to communicate the geometric extent of a Warning Area to a Warning System

$APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to an adjacent APS Area of Control without manual interaction

$APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to adjacent legacy signalling system without manual interaction

$APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to adjacent track section, not equipped with any signalling system

$APS shall ensure that the transition of a train unit movement between two Area of Controls does not require stopping the train unit

$APS shall ensure that the transition of a train unit movement between two Area of Controls does not reduce the operationally required maximum speed of the train unit

$APS shall support transitions from and to neighbouring areas equipped with lineside signals located at the border either in the own AoC or in the neighbouring area

$Default configuration shall contain values which can be changed within an unambiguously defined range to adapt to an IM’s requirements

$ APS must ensure that erroneous configuration data changing a default configuration does not disable the corresponding safety check

$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) during any installation procedure

$APS subsystem software approval must be possible independent of configuration data

$APS hardware and software approval must allow 1:1 exchange as maintenance activities within the authorisation for placing on the market or placing in service

$Identification of an incompatible version/built (transport, marshalling, application model) shall be revealed (e.g. towards Monitoring) and must not violate the RAMS and the non-functional requirements

$APS shall support the exchanging of interfaced subsystems/ component during runtime without affecting the RAMS conditions of APS and without a need to restart any other subsystem/component

$APS shall be developed in such a way that it can be used independently of the life cycle of the runtime environment

$Build a system that is capable of handling the highest RAMS and non-functional Requirements of an IM

$APS shall support the deployment of a scalable system

$APS shall enable by configuration to consider different data volumes processed in a certain time and use different frequencies e.g. for demand of update of cyclic data without a need of change on the code/algorithm

$Define formal values / value ranges for each RAMS and non-functional requirement in combination with the corresponding runtime environment (e.g. hardware, operating system)

$Build an APS that can handle the highest RAMS and non-functional requirements as a sum of all agreed needs of different IM

$APS shall enable by configuration to consider different data volumes processed in a certain time and use different frequencies e.g. for demand of update of cyclic data within the limits of the RAMSS specification of the default configuration

$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) in the course of any installation procedure

$Identification of an incompatible version/built (transport, marshalling, application model) shall be revealed (e.g towards Monitoring) and must not violate the RAMS and the non-functional requirements

$APS shall support exchanging subsystem software versions during runtime without affecting the RAMS condition of APS and without a need to restart any other subsystem/component

$APS safety reactions shall be unambiguously specified

$APS shall provide a set of safety reactions, the IM can choose for implementation for handling of specific situations on the needs of the IM based on the specific safety case of the trackside system integrated by the IM

$APS shall support the configuration of values within value ranges for specific safety reactions for each identified safety violation

$APS shall consider customisable system parameters following national rules and laws, e.g. speed allowed in certain situations

$APS must enable or disable distinctive functions if they are not allowed to be used by national operational rules by keeping other distinctive core function present

$APS shall expect that each Map Data delivery encompasses the entire fail-safe track network topology according to the application conditions of the entire Area of Control

$APS shall expect that each concerning Edge terminates at a dedicated Node at the spot location of an Area of Control border

$APS shall expect a Map Data delivery as a list of new, changed and deleted topology objects in order to support updating its operating state

$APS shall support the unambiguously specified Map Data and its semantics

$APS shall expect that each Map Data delivery that differs from a previous delivery has a unique identifier in order to distinguish an update from a re-delivery

$APS shall expect that each Map Data delivery is received unchanged from the source

$The behaviour of the individual APS components shall be unambiguously specified

Annex C: Relation to the overarching A.P.M objectives

The objectives concerning all three subsystems (MAP, PE, APS) are grouped into the categories presented in the following chapters according to. The concepts and solution approaches presented in the previous chapter are aligned to the overall concept for A.P.M., thus the previously defined system requirements also fulfil the A.P.M. objectives. For the sake of completeness, the following sections provide the tracing to previously derived system requirements.

Standardisation, Automation and Integration

Objective	System Requirements
A.P.M.@Accompanying standardisation to reduce system compatibility testing between onboard and trackside	$All APS interfaces should be specified in an unambiguous, exact and testable way
A.P.M.@All building blocks shall utilise an identical MAP data reference, provided by each MAP data version in order to prevent interpretation efforts	$APS shall support the unambiguously specified Map Data and its semantics $APS shall expect that each Map Data delivery that differs from a previous delivery has a unique identifier in order to distinguish an update from a re-delivery $APS shall ensure that the application code only works on abstract representation of the topology $APS shall use a unified and generic representation of identified track occupancies, independent of the localisation technologies used
A.P.M.@Allow large area of control segment sizes to reduce the amount of transitions to neighboring legacy systems in order to reduce integration efforts	$APS shall support the segmentation of MAP data from interfacing systems
A.P.M.@Consider open interfaces to integrate as much formats as possible	$All APS interfaces shall be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact and testable way $The behaviour of the individual APS components should be formally specified when formal validation requires it $All APS specifications shall be freely available to anybody at no cost $All partners shall sign an open-source agreement at the very beginning of the project $All contributions to APS specifications fall under the agreed open-source agreement $No participant may claim any rights to the APS specifications or further work results openly published under the agreed open-source licence
A.P.M.@Deployment of the system must be possible in various configurations but all of them need to fulfil basic requirements	$APS shall provide a default configuration that allows safe movements on any railway network topology that complies with the defined application conditions
A.P.M.@Encapsulate minimal viable functionalities in building blocks to enable an individual configuration of the building blocks and simple interfaces	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block
A.P.M.@Integrate upwards compatibility by design	$APS must ensure Engineering Data independent approval $APS must ensure Software-independent approval $APS must ensure Hardware-independent approval

Objective	System Requirements
A.P.M.@Reduce complex and manually triggered or processed process and replace or reengineer with automated processes	$APS shall support and provide guidance for manual operation on a fallback user interface $APS shall support the transfer of Safety Responsibility in an automatic way $APS shall consume MAP data updates during runtime $APS documentation shall be generated automatically and stored in an efficient document management system $All APS interfaces must provide multi version support $APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol) $APS shall support the automatic identification and recognition of different system configurations and versions during runtime $APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime $APS shall recover efficiently after a reboot
A.P.M.@Reduce the number of individual systems, components, field elements sharing non-standardised interfaces	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block $APS shall support the automatic transition of a moving train unit from and to an APS Area of Control to an adjacent APS Area of Control without manual interaction
A.P.M.@Standardize all main CCS processes, functionalities and interfaces	$All APS interfaces shall be defined with unambiguous semantics $All APS interfaces should be specified in an unambiguous, exact and testable way
A.P.M.@Support a broad applicability to different railways and in various types of traffic and operational processes	$APS shall provide a set of safety reactions, the IM can choose for implementation for handling of specific situations on the needs of the IM based on the specific safety case of the trackside system integrated by the IM $APS must support the configuration of safety conditions according to an IM's needs
A.P.M.@Use interfaces with automatic adaptions and internal intelligence for interfacing different versions of building blocks without the need of upgrade existing building blocks based on change in interface	$All APS interfaces must provide multi version support $APS shall support the automatic identification and recognition of different system configurations and versions during runtime $APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime
A.P.M.@Use secure standard protocols	$APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)
A.P.M.@Use standardized processes and systems	$APS shall be developed using a robust software development process according to CENELEC standards $All APS interfaces should be specified in an unambiguous, exact and testable way
A.P:M.@Implement ATO GoA2 or GoA3-4	$APS shall support the transfer of Safety Responsibility in an automatic way
A.P.M.@Support fast module replacement	$All APS interfaces must provide multi version support $APS shall support the automatic identification and recognition of different system configurations and versions during runtime $APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime

Life Cycle Management and Updateability

Objective	System Requirements
A.P.M.@Asset management must support the demand for high-cadence asset modification	$The combined use of functional building blocks shall not require an additional safety assurance $The combined use of functional building blocks shall not require an additional safety assurance $The integration of building blocks with their own safety assurance shall result in a safe system that does not require further safety approvals. $APS shall not require an adaptation of the infrastructure when put into operation $APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations
A.P.M.@Build a modular system architecture that supports different lifecycles	$Ensure an agreed and committed life cycle policy between all suppliers for investment protection $All APS interfaces must provide multi version support
A.P.M.@Enable changes, adaptations and extensions throughout the life cycle of the building blocks	$All APS interfaces must provide multi version support $Future sematic changes shall under no circumstance require changes in the interfaces $APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)
A.P.M.@Exchangeability between building blocks must be present wherever non-overlapping technology lifecycle profiles are present	$APS building blocks shall work independently of the functionality of neighbouring blocks, therefore no assumptions about dedicated behaviour shall be made $APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations

Robustness

Objective	System Requirements
A.P.M.@Handle internal failures and degraded modes efficiently	$APS shall disclose and support the handling of internal failures
A.P.M.@Malfunctioning of system components shall not lead to a shutdown of the system	$APS shall disclose and support the handling of failures from interfaced RCA SubSys $APS shall support and provide guidance for manual operation on a fallback user interface $APS shall support the transfer of Safety Responsibility in an automatic way
A.P.M.@several modes for degraded operation ensuring a high-level of safety and a high-level of operational system must be implemented by design	$APS shall support and provide guidance for manual operation on a fallback user interface $APS shall support the transfer of Safety Responsibility in an automatic way
A.P.M.@The overall system should be as robust as possible against version changes and missing information	$APS shall be able to process information of varying quality on its interfaces
A.P.M.@Support of self/remote diagnostics	$APS shall disclose and support the handling of failures from interfaced RCA SubSys

Objective	System Requirements
	$APS shall support the transfer of Safety Responsibility in an automatic way

RAM Strategy

Objective	System Requirements
A.P.M.@Architecture design reduces the functional and non-functional dependencies between the SubSys and thus reduces the functional and non-functional requirements (especially RAMS) for the individual SubSys.	$Any functionality not declared safety-relevant shall be realised out of scope from APS $Safety checks shall be independent of operational procedures
A.P.M.@Demonstrably successful best practices in software development for highly available systems should be applied	$APS shall be developed using a robust software development process according to CENELEC standards
A.P.M.@Provide data about system behaviour about RAMS and capacity usage to other systems	$APS shall provide quantities and frequencies of processed data towards Monitoring
A.P.M.@Reduce maintenance efforts by maximally reducing dependencies between building blocks	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block

Safety Strategy

Objective	System Requirements
A.P.M.@Apply a generic safety approach in encapsulating smallest possible safety relevant functions in building blocks that allow a separate safety assurance	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block $The combined use of functional building blocks shall not require an additional safety assurance
A.P.M.@Design a modular system architecture with small as possible amount of safety relevant components	$Any functionality not declared safety-relevant shall be realised out of scope from APS $Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block

Security Strategy

Objective	System Requirements
A.P.M.@ Avoid unnecessary authorisation by building trusted clusters	$Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block

Objective	System Requirements
A.P.M.@Ensure security by design for all SubSys and data flows according to RCA	$APS shall be developed using a robust software development process according to CENELEC standards $APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back
A.P.M.@Support the integration with state of the art identity and access management service	$APS shall be developed using a robust software development process according to CENELEC standards

Migration Strategy

Objective	System Requirements
A.P.M.@Allow different system layouts from decentralized to highly centralized safe computing with virtualization and container technologies, n-modular redundancy, fast disaster recovery, multi-tenant and multi-company cloud structures	$APS shall disclose and support the handling of failures from interfaced RCA SubSys $APS shall disclose and support the handling of internal failures $APS shall support and provide guidance for manual operation on a fallback user interface $Safety relevant functions shall be realised in small building blocks with as little input data as possible and simple (wherever possible binary) output to achieve a separate safety assurance for each building block
A.P.M.@Avoid temporary investments (e.g. avoid temporary interfaces between old and new interlockings by supporting technically the efficient and stable replacement of full lines by just replacing safety logic but not the OC)	$APS shall be interfaceable to a various number of present Object Controller in compliance to the EULYNX standards, interfaced to different legacy interlocking systems $APS shall support the safe movement of a train unit from an APS Area of Control to an adjacent legacy signalling system and vice versa $APS shall support the safe movement train units on an arbitrary railway network without major adaptations of existing trackside assets
A.P.M.@Provide scalable system architecture to be used in a modular way depending on local needs	$APS building blocks shall work independently of the functionality of neighbouring blocks, therefore no assumptions about dedicated behaviour shall be made $APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations

Usability

Objective	System Requirements
A.P.M.@Provide state of the art usability for GUI operations (incl. comfort functions such SSO)	TBD
A.P.M.@Allow integration of GUI for all APM systems, which allows a cross-system overview and quick change between operated systems	TBD

Objective	System Requirements
A.P.M.@Ensure synchronized state between GUI of all APM systems	TBD