RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

APS Detailed concepts overview

Document ID: RCA.Doc.52

Table of contents

1 Preamble

1.1 Release Information

Basic document information:

RCA-Document Number: RCA.Doc.52

Document Name: APS Detailed concepts overview

Cenelec Phase: 1

Version: 1.0

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

No disclaimer defined.

1.4 Purpose

See chapter 'Introduction'.

2 Version history

Version	Date	Author	Description
1.0	2022-09-30	Frank Skowron	First published version for RCA BL1 R0

3 Introduction

The Advanced Protection System (APS) is a core system inside the Reference CCS Architecture (RCA) that is generating business and operational requirements, an architecture description, functional, non-functional and interface specifications enabling further specification steps and specific implementations.

This document is part of a set of documents that will form the “APS concept”. While document levels 01 (with #business targets) and 02 (with @business objectives) - refer to section 1.3 Related documents - give the general motivation for a modern, future CCS from business perspective, document level 03 breaks these down to the $requirements to APS as part of RCA and already explains APS concepts on a coarse-grain level.

3.1 Purpose of this document

This document gives an overview on further documents which detail the documents on levels 01 to 03. The intention of their scope of topics is to concentrate on new ideas of RCA compared to current CCS systems.

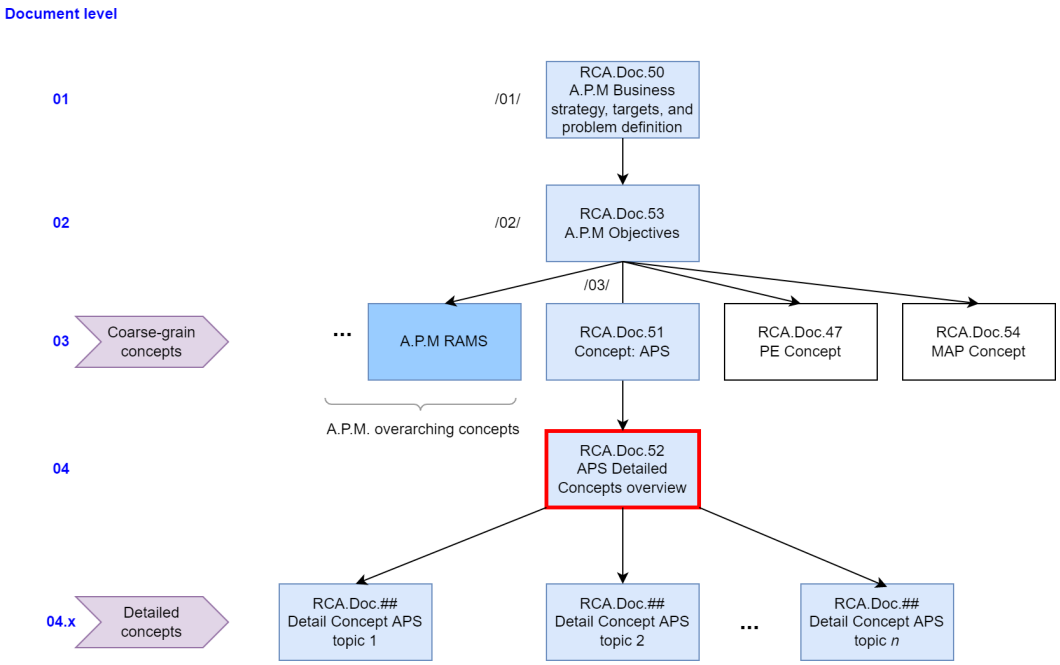
The detailed concepts shall be used for better understanding of APS. They will show that coarse-grain level concepts are realistic, and investigate and explain how the related challenges can be solved and will greatly help signalling engineers to capture the ideas behind APS.

Delimitation	These documents are not supposed to be specifications. These will be elaborated after the detail concepts have been finished and approved. Neither, they do not cover all topics, and topics themselves are investigated to a degree of current knowledge.

3.2 Intended readership

Intended readers are mainly signalling engineers both from infrastructure managers and i ndustry suppliers , particularly those who co-operate in ERJU's System Pillar and Innovation Pillar. Also OCORA stakeholders will find useful information about the trackside CCS.

3.3 Related documents



3.4 References

3.4.1 Non-normative documents

The following table lists all documents relevant for APS concepts. For the RCA documents amongst them, please refer to the RCA documentation plan /RCA.Doc.6/ for further details:

Reference	Document title
/RCA.Doc.6/	RCA Documentation plan
/RCA.Doc.14/	Terms and abstract concepts
/RCA.Doc.40/	RCA Architecture poster
/RCA.Doc.46/	Concept: Digital Map
/RCA.Doc.47/	Concept: Plan Execution
/RCA.Doc.50/	A.P.M Business targets and strategy
/RCA.Doc.51/	Concept: APS
/RCA.Doc.53/	A.P.M Objectives
/RCA.Doc.61/	APS Concept: Operating State and APS domain objects
/RCA.Doc.62/	APS Concept: Route setting and route protection
/RCA.Doc.63/	APS Concept: Movement Permission
/RCA.Doc.67/	APS Concept: Movable Object
/RCA.Doc.68/	Concept: Track Occupancy. Overall Solution Concept.
/RCA.Doc.69/	MAP Object catalogue
/RCA.Doc.70/	Concept: SCI-CMD
/RCA.Doc.79/	Position paper: Level crossings
/EULYNX_SCI-P/	EULYNX Interface specification SCI-P
/EULYNX_ReqP/	EULYNX Requirement specification for subsystem Point

3.4.2 Standards

(no references yet)

3.4.3 Regulations and Directives

Reference	Document title
/ SUBSET-026/	System Requirements Specifications for ETCS (Subset-026), latest official Version 3.6.0 in terms of Set of Specification #3 of TSI CCS
/ SUBSET-041/	Performance Requirements for Interoperability, Version 3.2.0
/ SUBSET-091/	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, Version 3.6.0
/IOP-Directive/	Directive (EU) 2016/797 on the interoperability of the rail system within the European Union
/TSI OPE/	Technical specification for interoperability relating to the operation and traffic management subsystem of the rail system in the European Union, current version (EU) 2019/773
/TSI CCS/	Technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union, current version with amendment (EU) 2019/776

3.5 Terms and abbreviations

(needed to understand APS, compare also /RCA.Doc.14/)

#

Prefix to identify a business target (from /RCA.Doc.50/)

@

Prefix to identify a business objective (from /RCA.Doc.53/)

$

Prefix to identify a requirement (from /RCA.Doc.51/)

Advanced Protection System, Plan Execution, Map (A.P.M)

APS, PE and Map are core subsystems of RCA and form together A.P.M.

Advanced Protection System (APS)

A group of subsystems in the RCA interface architecture responsible for safe track usage and for control and supervision of the railway production.
APS assures as a gatekeeper, that the requests of Plan Execution (PE) create a safe traffic flow and then executes them.
It includes the proposed subsystems Safety Logic (SL), Safety Manager (SM), Object Aggregation (OA), Movement Authority Transactor (MT), Mobile Object Transactor (MOT) and Fixed Object Transactor (FOT)

Advanced Protection System Area of Control (APS AoC)

The Advanced Protection System Area of Control (APS AoC) is the topologically limited extent of the Advanced Protection System with its technical components covering the specific

infrastructural track assets in this area. The term is used here for defining the technical and operational responsibility of one Advanced Protection System (APS).

Please note: 1..n APS AoC might be mapped to 1 AoC.

Allocation Section (AS)

An Allocation Section (AS) is defined as a directed Linear Contiguous Track Area of 1...n Track Edge Sections and 1..n exclusive dependencies as additional information.
The direction always leads away from the dependent Allocation Section (from conflict area to non-conflict area of clearance gauge).
Allocation sections are located in Track Areas where one or more clearance gauge conflicts between different tracks arise.

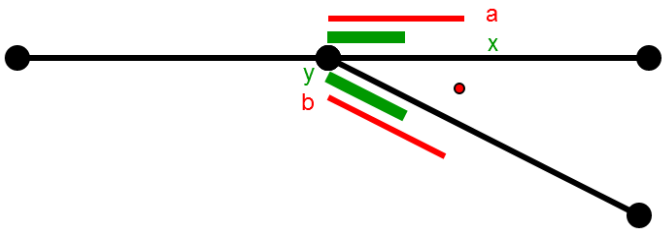
The conflict arises when the clearance gauges of different tracks overlap each other.
Out of this conflict an exclusive, symmetric interdependency between two or more Allocation Sections has to be deduced.
Exclusive dependency means that if one allocation section is fully or partially occupied by a Movable Object or if it is fully or partially contained in a granted Movement Permission Extent, no Movement Permission may be granted over any dependent Allocation Section.
Allocation Sections may overlap each other. In this case there must not be an exclusive dependency between the overlapping Allocation Section.

A non-complete list of usages is: points, diamond crossings, single and double slips, turnouts and gauntlet tracks.
All use cases and the according modelling principles can be affiliated to three basic assets: a diverging of Track Edges in a Track Node (point), a crossing of Track Edges (diamond crossing) and an interlacing track edges or there clearance profile (gauntlet).

Note: In the following figures, red and brown denotes an Allocation Section and green denotes a Drive Protection Section.

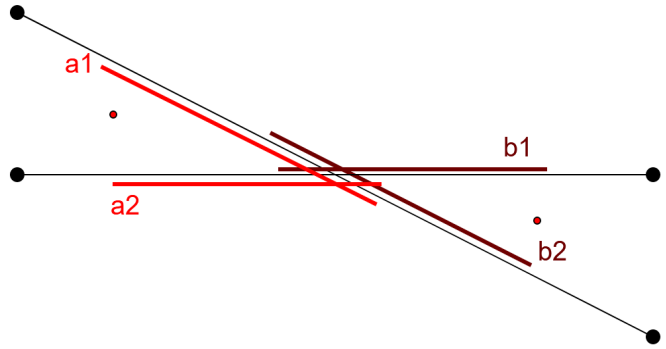
Example of a point

exclusive dependency: a <=> b



Example of a diamond crossing

exclusive dependencies: a1 <=> a2, b1 <=> b2



Automatic Train Protection (ATP)

Automatic train protection is a type of train protection system which continually checks that the speed of a train is compatible with the permitted speed allowed by signalling system, including automatic stop at certain signal aspects.

Cabin (cab)

The space in the power unit or driving unit of the train containing the operating controls and providing shelter and seats for the driver or engine crew /SUBSET-023/.

Change Request (CR)

A Change Request is a document containing a call for an adjustment of a system; it is of great importance in the change management process.

Control-Command and Signalling (CCS)

All the trackside and on-board equipment required to ensure safety and to command and control movements of trains authorised to travel on the network.

Digital Map (MAP)

RCA subsystem

Domain Object

A Domain Object is an abstract object for which a Domain (e.g. APS) has the main responsibility. There might be other Domains who are consumers of this object as well.

Drive Protection Section (DPS)

A Drive Protection Section (DPS) is defined through an extent on the track. It represents a part of a trackside asset that changes drivability. A Drive Protection Section is typically represented as one Track Edge Section where, for Physical Train Units to pass safely, a switchable field element has to be set to and secured in a specific position.

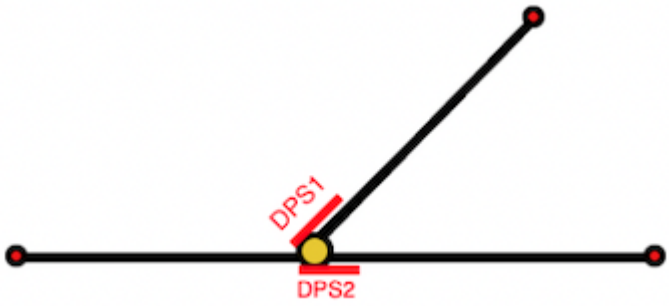
Note that the Drive Protection Section does not represent the switchable element itself but rather a part of the track, which - depending on the state of the switchable field element - is fully drivable (Full), limited drivable (Limited) or not drivable (None). Therefore one switchable field element may affect several Drive Protection Sections. A simple point has two Drive

Protection Sections for the two branching tracks and a level crossing has as many Drive Protection Section as tracks are passing through the level crossing. Common switchable field elements that require Drive Protection Sections are (non-complete list): Points, Level Crossings, derailers, movable bridges, gates, turntables.

Drive Protection Sections of the same physical elements have interdependencies - e.g. the two Drive Protection Sections of a simple point can not both be drivable at the same time. To indicate an interdependency, several DPS are grouped in one DPS Group (compare 'Drive Protection Section Group').

The following picture shows a simple point as an example of a switchable field element.

The following drawing shows the representation of the single tracks that are passing through the simple point as Drive Protection Sections. In addition, topology objects are shown to increase the understanding.

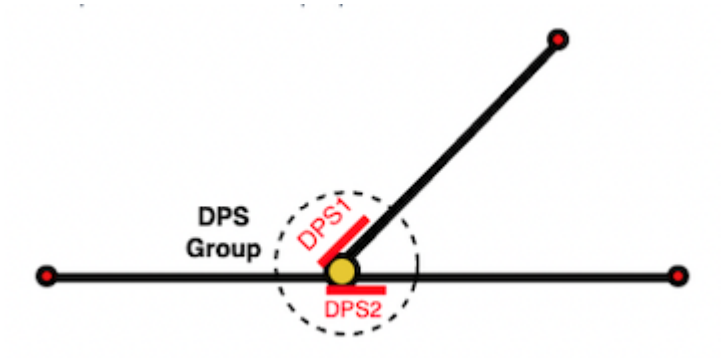


Drive Protection Section Group (DPS Group)

A Drive Protection Section Group (DPS Group) groups 1..n Drive Protection Sections which belong to the same switchable field element. DPS in one DPS Group might be dependent from each other. Furthermore, the DPS Group indicates the state of the switchable field element. Please note: a switchable field element (e.g. a slip point) might be represented by more than one DPS Group.

The following picture shows a simple point for which a Drive Protection Section Group is used as the Domain Object for representation.

The following drawing shows the representation of a simple point as a Drive Protection Section Group.



Europe's Rail Joint Undertaking (ERJU)

European Union Agency for Railways (ERA)

The European Union Agency for Railways (ERA) is established to provide the EU Member States and the Commission with technical assistance in the development and implementation of the Single European Railway Area. www.era.europa.eu

European Train Control System (ETCS)

The European Train Control System (ETCS) is the signalling and control component of the European Rail Traffic Management System (ERTMS). It is a replacement for legacy train protection systems and designed to replace the many incompatible safety systems currently used by European railways. ETCS is specified at three numbered levels (x = 0, 1, R).

ETCS End of Mission

ETCS End of Mission (EoM) refers to the situation where the trackside stops to authorise the movement of a Train Unit. It is initiated by the on-board equipment or Train Driver in order to

finish the specific train run. ETCS EoM can be indicated by entering a specific mode of the train control system.

EULYNX

EULYNX is an European initiative by 13 Infrastructure Managers to standardise interfaces and elements of the signalling systems. Aiming for defining and standardising interfaces in the future digital control command communication, signalling and automation system, the goal is a significant reduction of the lifecycle cost.

Facing (point direction)

The direction in which there is a choice of diverging destination.

Handing Over Area of Control (HOV AoC)

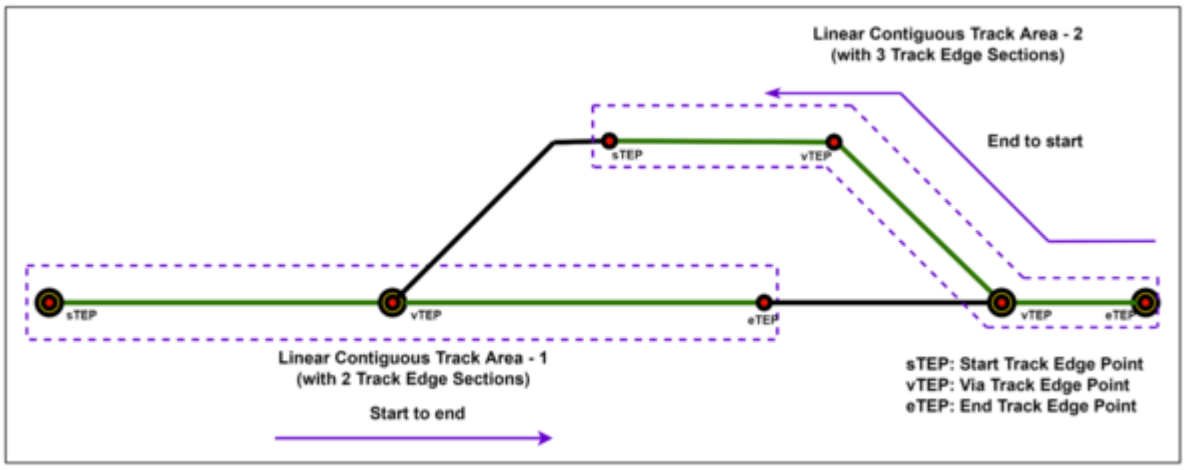
Area of Control from which a handover is performed to the neighbouring area.

Last relevant balise group (LRBG)

The LRBG is used as a common location reference between the ERTMS/ETCS on-board and trackside equipments in level Rs 2 & 3 /SUBSET-023/.

Linear Contiguous Track Area (LCTA)

The Linear Contiguous Track Area is a specialized class of Track Area to group an ordered and directional number of topologically connected Track Edge Sections such that they form exactly one path. The sequence of sections needs to be unambiguously navigable along the track network. Meaning that, each end of a Track Edge Section coincides with the start / end of the immediately succeeding section in the sequence.



Level R

Radio-based ETCS level

Max Safe Front End (maxSFE)

The Maximum Safe Front End position differs from the estimated position by the under-reading error of the localisation system.

Movable Object (MOB)

A Movable Object (MOB) is a representation of a real-world object as part of the physical railway system that moves. Such Movable Objects can be trackbound (such as Physical Train Units) or non-trackbound (such as Authorised Trackside Persons).
Any real-world movable object which is detected as such by a person or system with safety responsibility will be represented as a Movable Object in System RCA.

Movable Object extent

The Movable Object Extent (MOB Extent) represents the safe extent of the corresponding object in the Topology. It consists of the navigable gap-free and overlap-free path between two Track Edge Points. For determination of the MOB Extent, different sources of information are used. For Resolved Trackbound Movable Object it results for example from a combination of Train Detection System information with reported front and rear end position as well as the path in between under consideration of inaccuracy of the localisation technology.

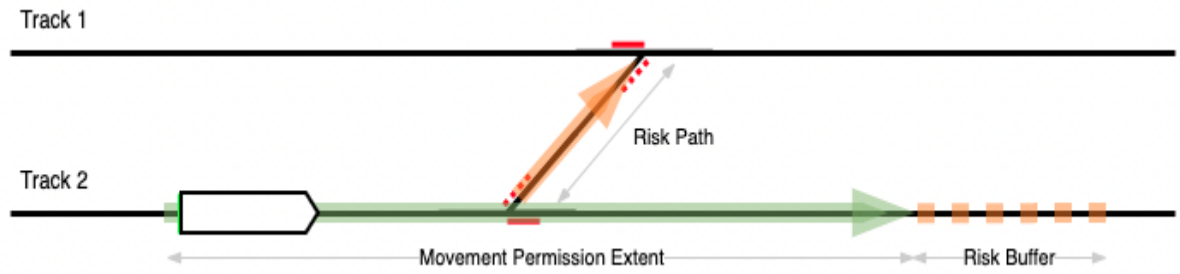
Movement Authority (MA)

Permission for a train to run to a specific location within the constraints of the infrastructure / SUBSET-023/.

Movement Permission (MP)

A Movement Permission (MP) is an authorisation for a particular Trackbound Movable Object to move in a defined direction, with a defined maximum speed profile, along a defined path (a Linear Contiguous Track Area) on the track network represented as so-called Movement Permission Extent plus safety margins (Risk Path(s) and Risk Buffer). A Movement Permission includes all conditions under which the movement of the Movable Object can be performed safely. A Movement Permission always refers to exactly one Movable Object.

Example of a Movement Permission:



Movement Permission extent

The Movement Permission Extent (MP Extent) is a Linear Contiguous Track Area in a defined direction. It describes the topological extent of the running path of the Movement Permission.

Non Trackbound Movable Object (nMOB)

Identified and localised objects such as Contruction Equipment or Authorised Trackside Persons are represented as Non-Trackbound Movable Objects. The movement of these objects is not constrained along the paths defined in the railway network Topology domain.

Object Controller (OC)

see EULYNX

Occupancy claim

An occupancy claim is the claim from a domain object to a segment of the abstracted railway track, which blocks or limits the track path usage. This includes for example:

- Track occupancies (caused by Movable Objects) - derived from trackside train detection and on-board localisation technologies;
- Track path claims/reservations (Movement Permissions);
- Track path restrictions (Usage Restriction Areas, Warning Areas).

Operating State: APS Operating State

The APS Operating State is the representation of the actual state of the physical railway system in the Area of Control of APS.

Onboard Train Detection (OTD)

Onboard Train Detection (OTD) is the abstract term for detection of rolling stock on a track where the detection technology is placed onboard.

Onboard Train Detection Area (OTD area)

Contiguous Track Area where OTD is used. A TTD is either not present at all or non-contiguous (for support of OTD) only.

→ Non-OTD equipped rolling stock cannot be detected in all tracks and will usually not be admitted to an OTD area.

Planning System (PAS)

Planning System provides functionality for preparing and optimising the entire schedule within an Area of Control. This schedule will be represented by Missions for Train Units. Missions are provided to System RCA where they enable command and control of traffic operations. System RCA provides the current operation state to the Planning System as feedback.

Plan Execution (PE)

Full name Plan Execution. Subsystem PE is a railway control and monitoring system. The core functionality of Subsystem PE is the automatic and efficient processing of the Operational Plans sent by the external Planning System (PAS) for implementation to Subsystem SL.

- Subsystem PE implements operational movements by timely requesting movement permissions for train units and state of Field Elements for the driveability of the railway network from Subsystem SL.
- Subsystem PE implements operational restriction areas and operational warning areas by timely requesting these areas from Subsystem SL.

The scope of Subsystem PE's functionality is still under consideration.

All of this core functionality is based on the knowledge of the Operating State, a safe logical representation of the actual state of railway operations in the area of control, which is provided from SL to PE via the Standard Communication Interface - Command (SCI-CMD), used by Subsystem PE and provided from Subsystem PE to Planning System outside the system border of RCA via the Standard Communication Interface - Operational Plan (SCI-OP).

As a connecting Subsystem between Planning System and Safety Logic (Subsystem SL), Subsystem PE makes a decisive contribution to RCA so that the overall system can benefit from new technical possibilities such as support of continuous localisation, moving block or geometric safety.

Characteristics:

- operates on abstract representations of real-world elements
- operates in real-time
- functions independently of business rules (business rules are expressed in the parameter values of Operational Plans and requests)
- provides functionality independent of the availability of Planning System (manual input via workbench)

Physical Train Unit (PTU)

Physical Train Unit (PTU) is physically existent, driveable and made up of a single or an ordered sequence of Physical Consists coupled together.

Physical Vehicle

Physical Vehicle is a physically existent, single item of rolling stock which is registered in the National Vehicle Register.

Radio Block Centre (RBC)

A centralised safety unit that receives train position information via radio and sends movement authorities via radio to trains.

Reference CCS Architecture (RCA)

RCA (Rreference CCS Architecture) is a harmonised reference architecture6 for the future railway CCS, with the main goal to substantially increase the performance/total cost of ownership ratio of CCS.

Resolved Trackbound Movable Object (rMOB)

A Resolved Trackbound Movable Object (rMOB) is a Trackbound Movable Object which is identified, i.e. there is a 1:1 mapping between the virtual object in the model and a Physical Train Unit.

Note: A Resolved Trackbound Movable Object represents an object which is known to the Advanced Protection System (identified), independent of the availability of localisation information, i.e. both objects with valid but also with unknown or invalid position are represented as rMOBs.

Risk-based approach/securing

Risk-based approach and risk-based securing are used as catchphrases. They describe that only the situational needed safety margins and safety mitigation measures are required for a route path, when the risk acceptance criteria are not met. For APS this considers

- unified general safety checks,
- setting parameters of safety checks on a risk-based approach by the Infrastructure Manager, and
- specific check conditions per safety checks depending on the present information per specific movement.

As an example, no mitigation measure against flank collision must be implemented, if any conflicting movement can be excluded by presence of sufficient information.

Risk Buffer

The Risk Buffer connects gap-free to the End of a Movement Permission (EoP) and describes the extent on the Topology that could potentially be occupied by the Resolved Trackbound Movable Object, if the risk mitigation achieved by the Automatic Train Protection is insufficient to keep the Resolved Trackbound Movable Object within its Movement Permission Extent.
The Risk Buffer is part of a Movement Permission.

Risk Buffer extent

The Risk Buffer Extent describes the extent of a navigable gap-free and overlap-free Track Area of the Risk Buffer on the Topology in a defined direction.

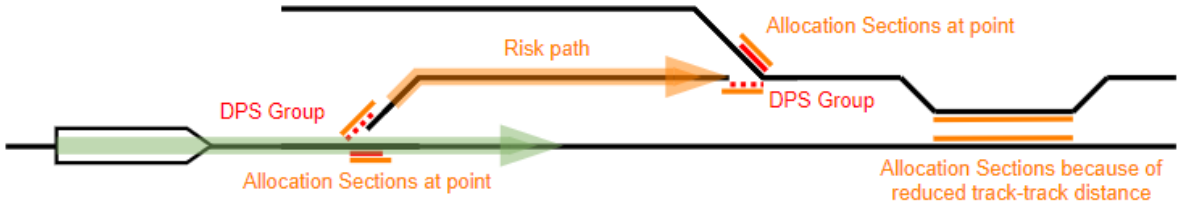
Risk Path

The Risk Path is one potential path by which a non-permitted vehicle movement could result in a flank collision with a vehicle moving along the Movement Permission extent.

The Risk Path starts at each end of the relevant Allocation Section in the extent of the Movement Permission (including the Risk Buffer, if not opted out by other configuration) and is limited through a sufficient method for providing flank protection.

For instance, a Drive Protection Section Group or Movement Permission could be used for limiting the Risk Path.

The Risk Path is defined as a Contiguous Track Area.



Route Path

The route path describes the specific topological extent for a specific planned movement within an Area of Control. The route path covers two main parts:

- the running path: description of the used infrastructure and
- the safety margins.

Note: It is not explicitly given, that route refers to the route concept in legacy interlockings with start and end at a signal. This is based on the overall usage of the term "route" within the /IOP-Directive/ and the /TSI OPE/ for description of the infrastructural view for enabling the operational planning of so-called train paths.

Route Path clearing

Route path clearing is the specific check of freedom of unpermitted occupations of the route path according defined rules. The term applies independent from the technical solution to be used and covers the running path and the safety margins.

Note: Specific parts where the route path clearing is used, are indicated e.g. the Movement Permission Extent.

Safe train length

The safe train length information shall represent the distance between the min safe rear end (by subtracting the train length from the min. safe front end position at the time when integrity

was established last time) and the estimated position of the train front / SUBSET-026-3/-§3.6.5.2.4.

Safety Integrity Level (SIL)

State machine

A state machine is the representation of the Model Based Systems Engineering process behaviour. It describes any subsystem functionality unambiguously, concisely and completely; as opposed to sequence diagrams which only represent individual (sub)scenarios and do not specify the dependencies between the functions and different use cases.

Technical Specification for Interoperability (TSI)

The Technical Specification for Interoperability (TSI) are specifications drafted by the European Railway Agency and adopted in a decision by the European Commission, to ensure the interoperability of the trans-European rail system. The interoperability issues apply to the lines within the Trans-European Rail network.

Trackbound Movable Object (tMOB)

A Movable Object whose movement is strictly bound to the paths defined by the railway network Topology domain (that is, a Movable Object that is guided by the rails). Trackbound Movable Objects are distinguished between Unresolved Trackbound Movable Objects and Resolved Trackbound Movable Objects.

Track Occupancy

A Track Occupancy is a representation of an area of the track (with possible zero extent) that is either occupied by a railway vehicle, construction equipment or by authorised railway staff or for which cannot be excluded that it is occupied by such an object. A Track Occupancy is defined by at least one position (i.e. a Track Edge Point in the topology), an extent and an optional safety margin.

Train Integrity

The level of belief in the Train Unit being complete and not having left coaches or wagons behind.

Train Integrity Monitoring (TIM)

The abstraction of functional capabilities of a Train Integrity Monitoring System, which is a device or a technology located onboard to monitor integrity of a dedicated physical train unit and provide information about the integrity state.

Trackside Train Detection (TTD)

Trackside Train Detection (TTD) is the abstract term for detection of rolling stock on a track, where the detection technology is placed trackside. Trackside Train Detection is provided in the scope of RCA by EULYNX Train Detection System

Trackside Train Detection Area (TTD Area)

Contiguous Track Area where a Trackside Train Detection is contiguously present and used.

→ Non-OTD equipped as well as OTD equipped rolling stock can be detected in all tracks and therefore will be admitted to a Trackside Train Detection area.

Track Vacancy Proving Section (TVPS)

According to EULYNX Eu.Doc.9 a Track Vacancy Proving Section (TVPS) is a portion of track which the Interlocking system can recognise by means of a track vacancy proving system. In scope of RCA the TVPS state is no more evaluated by an Interlocking. A Track Vacancy Proving Section (TVPS) will be understood in scope of RCA as a portion of the track which the trackside system can recognise as occupied or vacant by means of a Trackside Train Detection (TTD) system.

Union Industry of Signalling (UNISIG)

Union Industry of Signalling (UNISIG) is a working group of UNIFE with the goal to create the ERTMS/ETCS specifications.

Unresolved Trackbound Movable Object (uMOB)

Represents Trackbound Movable Objects which is not (yet) identified, i.e. there is no 1:1 mapping between the virtual object in the model and Physical Train Units (PTUs).

In case of using a Train Detection System this occurs when a track section is occupied. An Unresolved Trackbound Movable Object may in reality represent zero up to several separate unregistered PTUs in the same Track Vacancy Proving Section (TVPS).

In areas without a Train Detection System installed, this can occur as a consequence of degraded situations. APS defines then an occupation extent by performing an internal calculation.

Notes:

- A track section can also be occupied in case there is no PTU located, but a disturbance of Train Detection System is given.
- Strictly speaking, an Unresolved Trackbound Movable Object therefore only exists in case of missing knowledge that cannot be resolved by APS itself.

Usage Restriction Area (URA)

A Usage Restriction Area (URA) limits or constrains movements on an area described by an overlapping free but not necessarily connected set of Track Edge Sections.
Usage Restriction Areas can be created according to an Operational Plan (e.g. for enabling construction works) or in response to an Incident (e.g. as a mitigation measure). Various

limitations are possible for Usage Restriction Areas e.g. speed reduction or full track closure. Under certain conditions, a Movement Permission may overlap a Usage Restriction Area (e.g. construction vehicle must enter a construction site). Usage Restriction Areas can overlap, for example when multiple construction sites overlap or specific limitations apply to the same location.

Warning Area (WA)

A Warning Area is described by a TrackArea in which Authorised Trackside Person must be protected while performing trackside works.

The Warning Area is related to a collective Warning Subsystem (light and sound) and/or an individual Warning Subsystem (light, sound, and vibration).

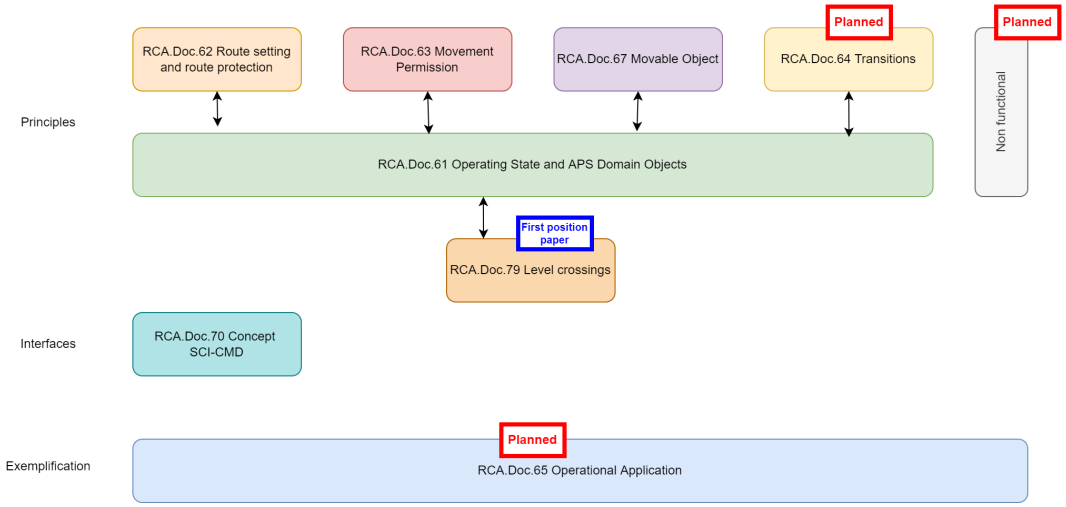
These warning subsystems are activated when a Movement Permission is intersecting with the Warning Area AND the Trackbound Movable Object of the Movement Permission is approaching a defined entry point. These devices are deactivated when the (rear end of) the Trackbound Movable Object has left a defined exit point.

---

4 APS detailed concepts

4.1 Overview

Detailed concepts can be grouped into the following categories:



First, general principles are elicited: The base for all static (topology) and dynamic (states) information is described in the Operating State . In order to prepare to move an object, the Route setting and route protection takes place. At this time, only the infrastructure base for a movement is set and protected. To actually safely perform a movement, a Movement Permission must be given (including further checks). Movable Objects are the key elements for these. Transitions describe how objects are registered with APS, or handed over to or from APS from/to another CCS system (including APS).

Second, Operational Application describes the application of the introduced principles for exemplification. From this part one would expect to check if typical situations are addressed, so Infrastructure Managers could check if their required operational situations are covered. It is not (yet) a complete collection but will grow in future.

Non functional topics (for example performance aspects) will be detailed in a later stage.

> Note
>
> The documents describe "solutions" in the problem space and rather not in the solution space - it shall not restrict the solution space and suppliers' diversity of ideas, nor competition.

4.2 Concept scope

Detail concepts on document level 04 shall

- describe the details, how $requirements can be fulfilled by APS
- trace to these $requirements
    - the tracing is performed 'top-down'
- elicit "solutions" (in problem space)
- concentrate on new and changed "solution" elements

- be concrete as to
    - what scenarios happen
    - which kind of messages will be exchanged (no bit-wise details)
    - what are basic functional requirements
- be still at a good abstraction level in order to leave room for implementation freedom and creativity of suppliers

but shall not be understood as interface or requirements specifications .

RCA.Doc.70 (SCI-CMD) results from the concepts on document level 04.

5 How to read APS concepts

5.1 Basic typography

Concepts are written such that they can be an input for later specifications (interfaces, functional and non-functional requirements). The following typography is used to allow for easy identification of such elements in order to build later specifications:

Function	Identified needs for a behaviour of APS. The alternative term requirement is avoided as the description won't have the quality of a requirement, but requirements are expected to be derived from it.

Messages						
Interface	Name	Description	From	To	Parameter:Type	Remark
Messages between RCA subsystems. Parameters are described on a high level: high enough in order not to restrict the concrete solution but low enough to provide a good understanding how the message will work in a scenario. The message will be the base for a later definition of the respective SCI, where the missing details will unambiguously be fixed.						

Types		
Name	Description	Remark
Types of the used parameters. Again described on a high level (see remark for messages). The types will be the base for a later definition of the respective SCI, where the missing details will unambiguously be fixed.		

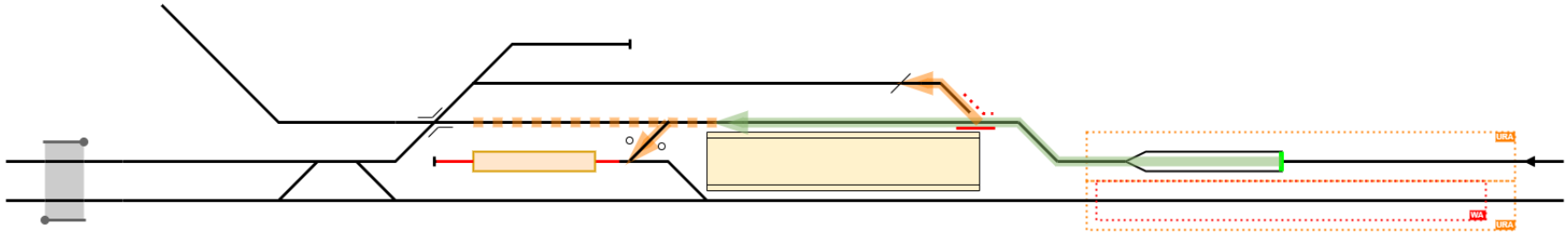
To be investigated	The named topic is known but not yet further investigated. Naming such topics should indicate that these have been identified and won't be forgotten.

Delimitation	The named topic is known but is expected to be not applicable. An example would be that APS is not responsible (strictly restricted to safety-relevant checks) but another RCA subsystem, and the topic has been identified and won't be forgotten.

5.2 Image typography

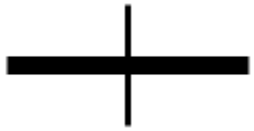
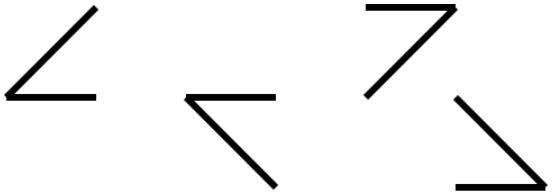
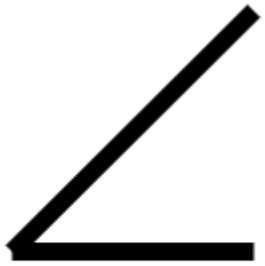
In order to follow a unique style, a set of symbols has been developed which are not explained in every concept, but centrally here.

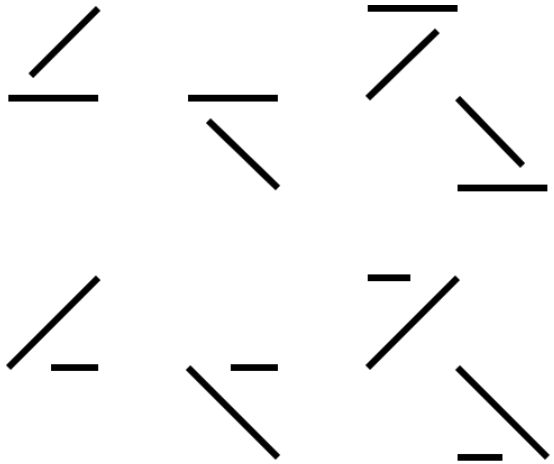
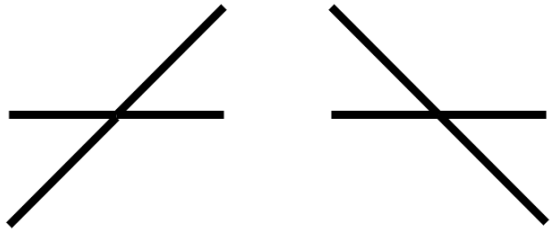
5.3 Example

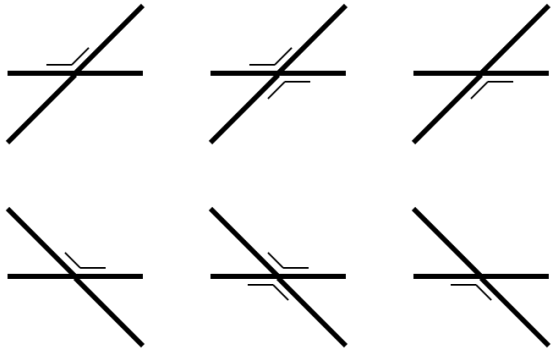
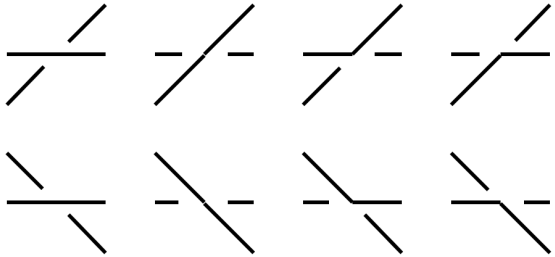
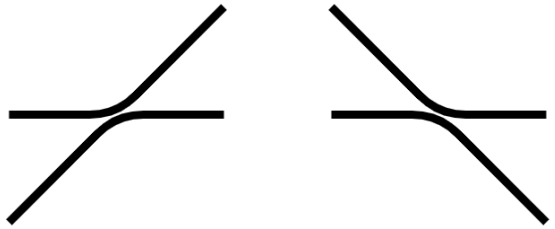


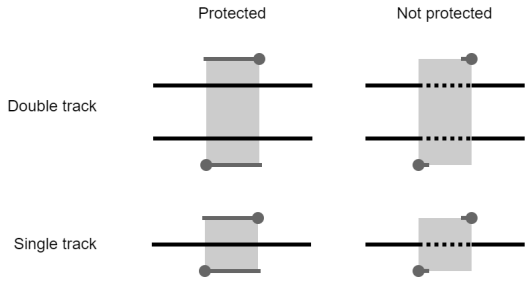
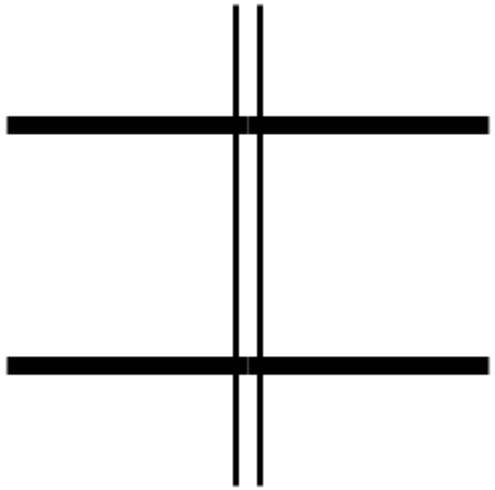
5.4 Template

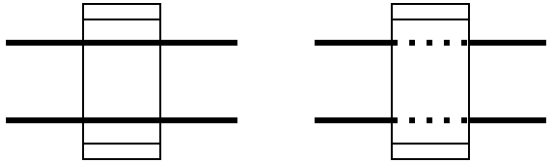
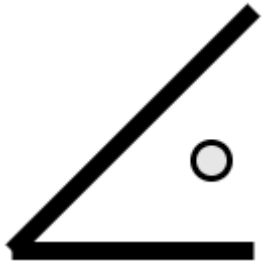
Entity	Representation	Remark
Infrastructure objects		
		If not mentioned otherwise, these settings are inherited by other entities
Main track		
Secondary track		
Occupied track		
Vacant track		

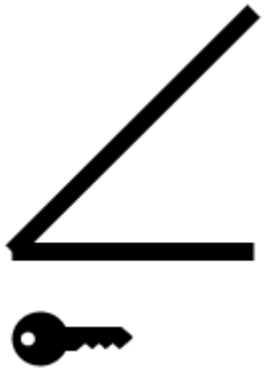
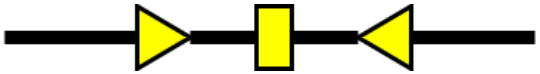
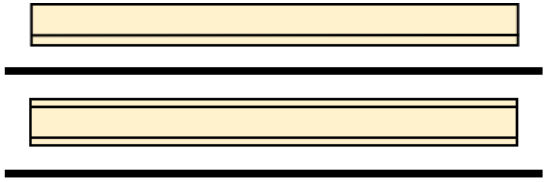
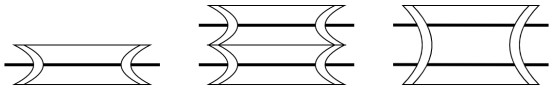
Entity	Representation	Remark
Infrastructure objects		
TTD border		
Buffer stop		
Point (irrelevant position)		
Locally operated point	 	
Point (relevant position)		

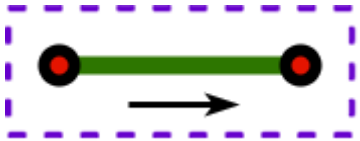
Entity	Representation	Remark
Infrastructure objects		
		
Crossing		
Slip point (irrelevant position)		

Entity	Representation	Remark
Infrastructure objects		
		
Slip point with outer tongues ("English slip points") (relevant position)		No need to distinguish single and double slips (thin lines ommitted)
Slip point with inner tongues ("German slip points", "type Bäsler") (relevant position)		

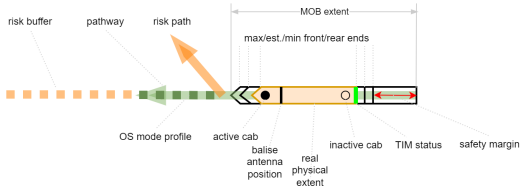
Entity	Representation	Remark
Infrastructure objects		
Derailer		Left image can be both used for irrelevant and relevant (detached) position; right image is attached position
Level crossing		Left images can be both used for irrelevant and relevant (protected) position; right image shall always be not protected
Gate		
Movable bridge		

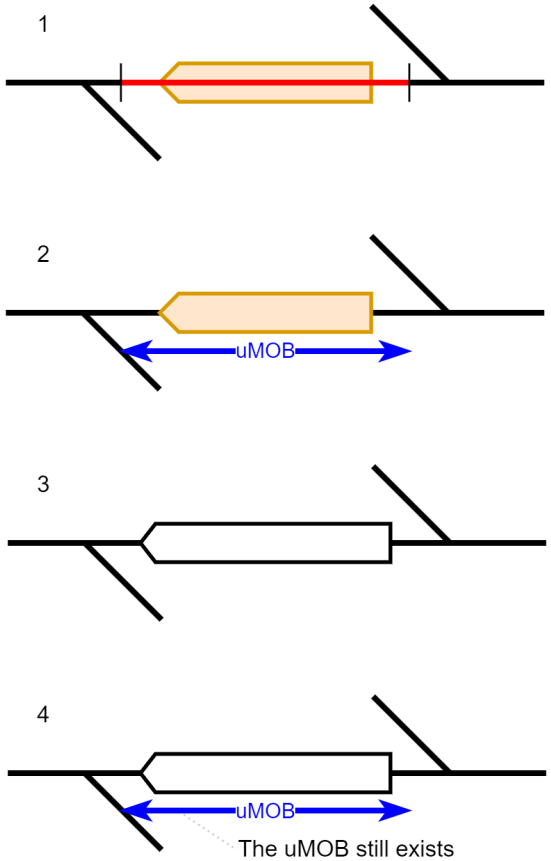
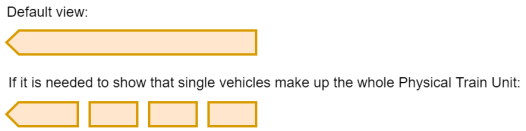
Entity	Representation	Remark
Infrastructure objects		
		Left image can be both used for irrelevant and relevant (closed) position; right image is opened position
Main signal (irrelevant aspect, stop aspect, proceed aspect)		The dotted line can be used to make the assignment to track unique (countries driving left, driving right, even deviations)
ETCS stop marker board		
ETCS location marker		
Fouling point		
Key lock		

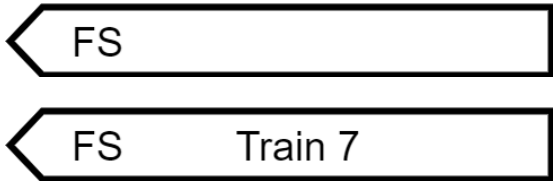
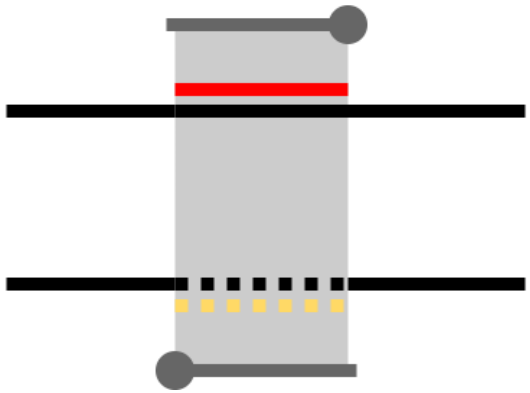
Entity	Representation	Remark
Infrastructure objects		
		Here in the example of a point. In general, the key symbol should be placed at the key-locked element.
Balise group		
Platform (one and two edges)		
Tunnel		
Abstract topology-related objects		
Track Node (type 'Point')		

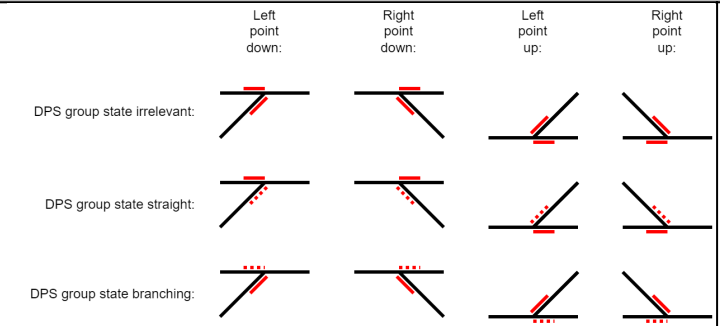
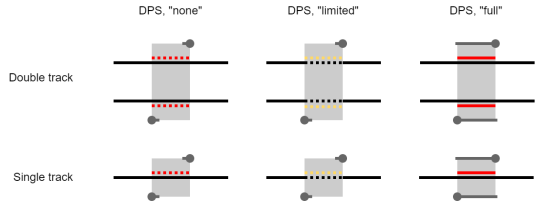
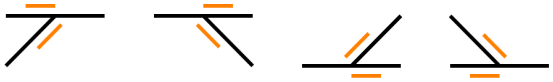
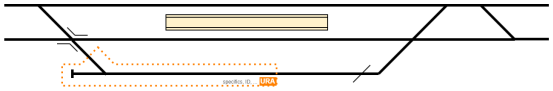
Entity	Representation	Remark
Infrastructure objects		
Track Node (type 'System border' or 'End of track')		
Track Edge with Track Nodes (type 'Point')		
Track Edge Point		
Track Edge Section with Track Edge Points		
Track Edge Point at the same location as Track Node (type 'Point')		
Area that includes several Track Edge Sections (Track Area, Contiguous Track Area, Linear Contiguous Track Area, Area of Control, Operational Point)	 Note: The dotted line rectangle is referred here.	
Area that includes several Track Edge Sections with a given direction		

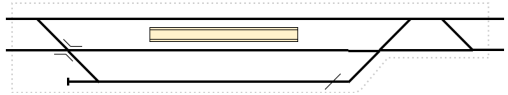
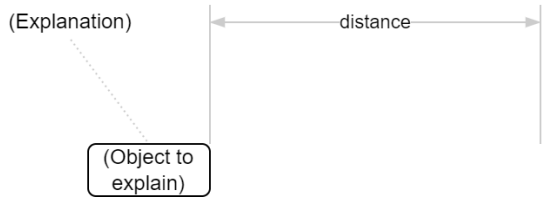
Entity	Representation	Remark
Infrastructure objects		
Movement Permission (MP)		
Running path		
Risk buffer		
Risk path		Orientation: points away from the fouling point to the protecting element
MP Request (not yet granted)		
Movable objects (MOB) and Physical Train Units (PTU) behind		
Resolved Trackbound Movable Object (rMOB)		
Unresolved Trackbound Movable Object (uMOB)	(see representation of track occupancy)	
All details		As the safety margin is included, the MP starts from the very right end.

Entity	Representation	Remark
Infrastructure objects		
	 Note: The TIMS endication is placed at the rear end of the MOB if the physical train extent (orange) is not shown	Assumption: the safety margin is considered part of the MOB which would ease drawings = attach MOB by MOB without a distance.
Example: just the rMOB		
Example: changing focus		1. There is an occupancy. In reality, it is caused by a physical train unit. It is depicted transparently in order to show the underlying occupancy of the TTD section, its TTD section borders are depicted 2. APS has created an unresolved trackbound MOB (uMOB) due to the detected occupancy, no further information is yet known. TTD-related information is no more in focus 3. The OBU has registered and information about position/length and direction is available (location inaccuracy = min/est./max ends not depicted) 4. If relevant, the still existing uMOB can be depicted in addition.

Entity	Representation	Remark
Infrastructure objects		
		
Physical Train Unit		

Entity	Representation	Remark
Infrastructure objects		
Additional information		
Non-trackbound MOB		
Control objects		
Drive Protection Section (DPS)	**Drivability states** **Appearance** FULL NONE LIMITED Application on points:	Note: Mixed drivability also possible 

Entity	Representation	Remark
Infrastructure objects		
	 Application on level crossings: 	
Allocation Section		
Usage Restriction Area (URA)		
Warning Area (WA)		
Area of Control (AoC)		

Entity	Representation	Remark
Infrastructure objects		
		If needed, an area shape like for URAs but with different colour can be used. This should only be needed if there is more than one AoC to be depicted.
Trackside Train Detection (TTD) area	Like URA	Depict it as any other area, use text label "TTD area" if needed
Onboard Train Detection (OTD) area	Like URA	Depict it as any other area, use text label "OTD area" if needed
Etc		
Measurements, Helper lines		Dashed lines to link an explanation to the explained object Helper lines to relate a measurement Restraint colour
Postponed (low priority)		
Turntable		
Traverser		

Annex: Requirement Tracing

The following table provides an overview of how many of the system requirements (leading with a "“$-symbol”) defined in /RCA.Doc.51/ are already addressed in the detailed APS concepts /RCA.Doc.61/,/RCA.Doc.62/, /RCA.Doc.63/ and /RCA.Doc.67/. The table serves as an indication if the $-requirements are addressed in any section (taged with a "§-symbol") of the detailed concepts but does not indicate if tehy are addressed fully or partially. Please note, that the $-requirements considered in the detailed concepts are not necessarily covered fully and that a formal, tool-supported requirements tracing will be implemented in future.

Chapter(s) in RCA.Doc.51	System Requirements derived in RCA.Doc.51	RCA.Doc.61 Operating State and APS Domain Objects	RCA.Doc.62 Route setting & protection	RCA.Doc.63 Movement Permission	RCA.Doc.67 Movable Object
Safety Checks	$All APS interfaces must be defined with unambiguous semantics				
Automation, Life Cycle Cost, Standardised interfaces	$All APS interfaces must provide multi version support				
Safety Checks, Generic product Assurance,Standardised interfaces, Functional independency, Managing Configurations	$All APS interfaces shall be specified in an unambiguous, exact and testable way				
Standardised interfaces	$All APS specifications shall be freely available to anybody at no cost				
Standardised interfaces	$All contributions to APS specifications fall under the agreed open-source agreement				
Standardised interfaces	$All partners shall sign an open-source agreement at the very beginning of the project				
Safety Checks	$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		§Configurability of behaviour	§Solution details	
Managing Warning Areas	$An IM shall have the possibility to configure the minimum and maximum pre-warning time			§MP in relation with WA	
Generic product Assurance, Functional independency	$Any functionality not declared safety-relevant shall be realised out of scope from APS		§Solution summary		§Attributes of Trackbound Movable Objects
Standardised interfaces	$APS building blocks shall work independently of the functionality of neighbouring blocks, therefore no assumptions about dedicated behaviour shall be made				§Life cycle of Movable Objects
Automation	$APS documentation shall be generated automatically and stored in an efficient document management system				
Generic product Assurance	$APS functions must be failsafe executable using any Map Data provided if the data complies to the application conditions				
Functional independency	$APS functions shall be failsafe executable using any Map Data provided if the data complies to the application conditions	§Geometric representation			
Managing Configurations	$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				
Standardised interfaces	$APS interface specification shall be detailed enough to enable a replacement of building blocks compliant to the same interface without further adaptations				
Managing Warning Areas	$APS must be able to communicate the geometric extent of a Warning Area to a Warning System				
Safety Checks	$APS must be able to identify safety condition violations		§Route clear checking	§Premises §Safety checks §MP granting	§General principles in the context of RCA
Managing Warning Areas	$APS must be able to issue Warning Commands in case of an identified runaway vehicle that may enter a working area				
Safety Checks	$APS must be able to transfer one or multiple of its safety responsibility to another authorised actor and back				

Managing Warning Areas	$APS must be able to update a previously issued Warning Command				
Managing Warning Areas	$APS must communicate with Warning Systems in order to send warnings and to receive acknowledgements				
Safety Checks	$APS must comply to defined safety conditions		§Functions		
Occupancy Claims Identifiable with Localisation Technologies	$APS must consider all usage restriction conditions of the track segments claimed for a movement			§MP restricted by URA §MP in relation with WA	
Managing Warning Areas	$APS must consider Warning Areas when granting movements			§MP in relation with WA	
Managing Configurations	$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		§Configurability of behaviour		
Generic product Assurance, Functional independency	$APS must ensure Engineering Data independent approval	§Abstraction			
Generic product Assurance, Functional independency	$APS must ensure Hardware-independent approval				
Generic product Assurance, Functional independency	$APS must ensure Software-independent approval				
Managing Configurations	$APS must ensure that erroneous configuration data changing a default configuration does not disable the corresponding safety check				
Managing Warning Areas	$APS must ensure that the Warning System has confirmed the Warning Command by APS before granting a movement			§MP in relation with WA	
Occupancy Claims NOT Identifiable with Localisation Technologies	$APS must ensure that URAs with safety relevance are not removed without adequate confirmation				
Managing Warning Areas	$APS must issue an individual Warning Command for each individual train unit			§MP in relation with WA	
Managing Warning Areas	$APS must make sure that prior to any movement within a Warning Area, an onsite warning – according to defined conditions - will be issued			§MP in relation with WA	
Safety Checks	$APS must not grant a movement when safety conditions are violated		§Functions	§Solution details	
Safety Checks	$APS must prevent collisions		§Functions	§Solution details	§General principles in the context of RCA
Safety Checks	$APS must prevent derailments		§Functions	§Solution details	
Managing Warning Areas	$APS must prevent that Warning Areas geometrically overlap				
Occupancy Claims NOT Identifiable with Localisation Technologies	$APS must represent any Map data in Operating State in a fail-safe way	§Fail-safe			
Safety Checks, Occupancy Claims Identifiable with Localisation Technologies	$APS must represent any track occupancy in a fail-safe way	§Abstraction §Fail-safe			§Determination of Trackbound Movable Object Extent
Safety Checks, Occupancy Claims NOT Identifiable with Localisation Technologies	$APS must represent any usage restriction in a fail-safe way	§Abstraction §Fail-safe		§MP restricted by URA	
Safety Checks	$APS must represent in real-time all granted movements in a fail-safe way	§Abstraction §Fail-safe $Real-time			
Safety Checks	$APS must represent in real-time all movable objects within its AoC in a fail-safe way	§Abstraction §Fail-safe §Real-time			§Attributes of Trackbound Movable Objects
Safety Checks	$APS must represent in real-time the current state of a switchable field element in a fail -safe way	§Abstraction §Fail-safe §Real-time	§Set switchable field elements		

Safety Checks, Occupancy Claims NOT Identifiable with Localisation Technologies	$APS must represent the operating state towards mobile devices in a fail-safe way				
Managing Configurations, Safety Checks	$APS must support the configuration of safety conditions according to an IM's needs				
Occupancy Claims NOT Identifiable with Localisation Technologies	$APS must support the confirmation of a URA removal from a mobile device				
Managing Warning Areas	$APS must support the reception of a Warning Command acknowledgement from the Warning System				
Managing Warning Areas	$APS must support the transmission of a Warning Command to a Warning System in the field				
Safety Checks	$APS must take one or multiple safety measures when a safety condition violation is identified				
Generic product Assurance	$APS risks shall be limited to safety-relevant aspects without considering business-critical risks to the railway performance	§Operating State in context of RCA			
Managing Configurations	$APS safety reactions shall be unambiguously specified				
Automation, Life Cycle Cost	$APS shall allow future syntax adaptations on the device abstraction and device control layer (e.g. new application protocol)				
Safety Checks	$APS shall allow movements under specific conditions, when localisation information becomes unavailable				
Safety Checks	$APS shall allow movements under specific conditions, when states of switchable field elements become unavailable				
Safety Checks	$APS shall allow the geometric overlap two route paths complying to the defined safety conditions				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall be able for interfacing new localisation technologies				§Solution approach, subchapter basic requirements
Occupancy Claims Identifiable with Localisation Technologies	$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				§Determination of Trackbound Movable Object Extent
Standardised interfaces	$APS shall be able to process information of varying quality on its interfaces	§Aggregation			§Attributes of Trackbound Movable Objects
Occupancy Claims Identifiable with Localisation Technologies	$APS shall be able to represent track occupancy using safe train length information	§Aggregation			§Resolved Movable Object Extent
Generic product Assurance, Functional independency	$APS shall be considered in the safety management process of RCA and be compliant with the safety requirements identified during the risk analysis				
Managing Configurations	$APS shall be developed in such a way that it can be used independently of the life cycle of the runtime environment				
Generic product Assurance	$APS shall be developed using a robust software development process according to CENELEC standards				
Life Cycle Cost	$APS shall be interfaceable to a various number of present Object Controller in compliance to the EULYNX standards , interfaced to different legacy interlocking systems		§Set switchable field elements		
Occupancy Claims Identifiable with Localisation Technologies	$APS shall be Safety Responsible for fail-safe granting movements to train units			$Solution details	
Generic product Assurance, Standardised interfaces	$APS shall consider all safety relevant railway network usage conditions prior to safely granting a movement for a train unit				
Managing Configurations	$APS shall consider customisable system parameters following national rules and laws, e.g. speed allowed in certain situations		§Configurability of behaviour		
Safety Checks	$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		§Configurability of behaviour	§Premises §Safety checks §MP granting	

Occupancy Claims Identifiable with Localisation Technologies	$APS shall consider safe train length information and integrity state for object aggregation for efficient track occupancy	§Aggregation			§Resolved Movable Object Extent
Safety Checks, Functional independency	$APS shall consider the provided Map Data as fail safe				
Safety Checks	$APS shall consider the safety conditions configured by an IM according to its requirements and regulations		§Configurability of behaviour	§MP granting	
Safety Checks	$APS shall consider to handle trains with continuous communication connection				§PTU with intergity (always reporting position) performs a mission with valid position
Automation	$APS shall consume MAP data updates during runtime	§Abstraction			
Automation	$APS shall continuously provide and monitor the current Operating State including during the initialisation phase, re-boot and after changing interfacing (sub-)systems				
Automation	$APS shall disclose and support the handling of failures from interfaced RCA SubSys	§Aggregation §Fail-safe	§Functions		
Automation	$APS shall disclose and support the handling of internal failures	§Fail-safe			
Managing Configurations	$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				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall enable operation without the need of installed contiguous trackside train detection system	§Abstraction	§Route clear checking		§Resolved Movable Object Extent
Safety Checks, Occupancy Claims Identifiable with Localisation Technologies	$APS shall enable operation without the need of lineside signalling system				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall enable track occupancy independently from fixed signalling blocks definition	§Geometric representation			§Resolved Movable Object Extent
Safety Checks	$APS shall encapsulate translation logic from processing logic	§Abstraction			
Standardised interfaces, Functional independency	$APS shall ensure that the application code only works on abstract representation of the topology	§Geometric representation §Aggregation			
Managing Transitions	$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				
Managing Configurations	$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	§Abstraction §Classification of APS Domain Objects into the MAP Object Model			
Managing Configurations	$APS shall expect that each concerning Edge terminates at a dedicated Node at the spot location of an Area of Control border				
Managing Configurations	$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	§Classification of APS Domain Objects into the MAP Object Model			
Managing Configurations	$APS shall expect that each Map Data delivery is received unchanged from the source	§Classification of APS Domain Objects into the MAP Object Model			
Managing Configurations	$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	§Abstraction §Classification of APS Domain Objects into the MAP Object Model			
Safety Checks	$APS shall implement a strict object aggregation, based on abstract concepts	§Aggregation			§Attributes of Trackbound Movable Objects
Safety Checks	$APS shall implement full supervision of shunting movements				

Occupancy Claims Identifiable with Localisation Technologies	$APS shall base the granting or rejecting of movement requests on track occupancy claims and field element states			§MP granting	
Safety Checks	$APS shall make the generic safety rules and the specific configuration data of the function make available for the operational level				
Safety Checks	$APS shall not consider any operational consequence when granting movements but solely if the movement is safe			§Premises §Safety checks §MP granting	
Safety Checks, Occupancy Claims Identifiable with Localisation Technologies	$APS shall not limit the start and end of movements to specific positions in the Area of Control			§Premises	
Safety Checks	$APS shall not prevent a movement of a train unit with unknown characteristics				
Standardised interfaces, Lyfe Cycle Cost	$APS shall not rely on the existence of localisation information from existing TTD systems to identify track occupancies				§Assumptions and prerequisites, subchapter Abstraction
Standardised interfaces	$APS shall not require an adaptation of the infrastructure when put into operation				§Assumptions and prerequisites, subchapter Abstraction
Occupancy Claims Identifiable with Localisation Technologies	$APS shall only support ETCS levels equal to or higher than L2				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall operate on different lines equipped with different ETCS level starting from Level 2				§PTU without integrity (not always reporting) performs SoM with valid position
Safety Checks	$APS shall prevent a train movement from exceeding a speed limitation within its defined geometric extent			§Premises §Safety checks §MP granting §Upgrading an MP	
Safety Checks	$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			§MP restricted by URA	
Standardised interfaces	$APS shall process localisation information from a variety of localisation systems and technologies	§Abstraction			§Assumptions and prerequisites, subchapter Abstraction
Standardised interfaces	$APS shall process localisation information from existing TTD systems	§Abstraction §Aggregation			§Assumptions and prerequisites, subchapter Abstraction
Occupancy Claims Identifiable with Localisation Technologies	$APS shall process mobile localisation device information of non-trackbound objects for aggregation of track occupancy				§Delimitations, subchapter Movable Objects
Occupancy Claims Identifiable with Localisation Technologies	$APS shall process mobile localisation device information of trackbound objects for aggregation of the track occupancy	§Abstraction			§Assumptions and prerequisites, subchapter Abstraction
Occupancy Claims Identifiable with Localisation Technologies	$APS shall process on-board localisation information for aggregation of the track occupancy	§Aggregation			§Assumptions and prerequisites, subchapter Abstraction
Managing Configurations, Independency from Project Planning	$APS shall provide a default configuration that allows safe movements on any railway network topology that complies with the defined application conditions				
Managing Warning Areas	$APS shall provide a functionality to create, change and delete geometric extents in Operating State, representing a Warning Area	§Geometric representation			
Managing Configurations	$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				

Independency from Project Planning	$APS shall provide identical functionalities for any kind of operational movements	§Abstraction			
Standardised 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				§Attributes of Trackbound Movable Objects
Life Cycle Cost, Standardised interfaces	$APS shall provide interfaces that are compliant to EULYNX interface specifications		§Set switchable field elements		§Solution approach, subchapter Basic requirements
Life Cycle Cost, Standardised interfaces, Safety Checks	$APS shall provide interfaces that are compliant to the TSI CCS				
Life Cycle Cost	$APS shall provide quantities and frequencies of processed data towards Monitoring				
Automation	$APS shall recover efficiently after a reboot				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall release each section of a secured route path after safely identifying its clearance based on train integrity information			§Shortening at rear end	§Resolved Movable Object Extent
Automation	$APS shall report errors and failures regarding incompatibilities between different system configurations and versions during runtime				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall represent any track occupancy as generic representation to be as independent as possible from formats of localisation devices	§Abstraction §Geometric representation			§Assumptions and prerequisites, subchapter Abstraction
Automation	$APS shall support and provide guidance for manual operation on a fallback user interface				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall support continuous localisation information to represent track occupancy	§Aggregation			§Resolved Movable Object Extent
Occupancy Claims Identifiable with Localisation Technologies	$APS shall support different ETCS levels simultaneously				§State machine of Resvolved Trackbound Movable Object
Standardised interfaces	$APS shall support different localisation technologies that may deploy different reference systems with different data formats on their interfaces	§Abstraction			
Managing Configurations	$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				
Safety Checks	$APS shall support FRMCS technology based communication technology for all communication purposes between onboard and trackside				
Safety Checks	$APS shall support GSM-R for a transition period				
Occupancy Claims Identifiable with Localisation Technologies	$APS shall support the aggregation of track occupancies along tracks not continuously equipped with trackside train detection system in conjunction with other localisation technologies	§Aggregation			vResolved Movable Object Extent
Automation	$APS shall support the automatic identification and recognition of different system configurations and versions during runtime				
Managing Transitions	$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				
Managing Transitions	$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				
Managing Transitions	$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			§MP at border/transition	

Managing Configurations	$APS shall support the configuration of values within value ranges for specific safety reactions for each identified safety violation				
Managing Warning Areas	$APS shall support the creation, change and deletion of a Warning Area to the authorised actors Plan Execution and human beings				
Managing Configurations	$APS shall support the deployment of a scalable system				
Managing Configurations	$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	§Abstraction			
Standardised 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				
Independency from Project Planning	$APS shall support the safe movement train units on an arbitrary railway network without major adaptations of existing trackside assets				
Standardised interfaces	$APS shall support the segmentation of MAP data from interfacing systems				
Safety Checks, Automation	$APS shall support the transfer of Safety Responsibility in an automatic way				
Managing Configurations	$APS shall support the unambiguously specified Map Data and its semantics	§Classification of APS Domain Objects into the MAP Object Model			
Managing Transitions	$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				
Standardised interfaces	$APS shall use a unified and generic representation of identified track occupancies, independent of the localisation technologies used	§Abstraction §Geometric representation			§Determination of Trackbound Movable Object Extent
Occupancy Claims Identifiable with Localisation Technologies	$APS shall use on-board localisation information for aggregation of the track occupancy				§Resolved Movable Object Extent
Occupancy Claims Identifiable with Localisation Technologies	$APS shall use train integrity information provided by on-board or trackside for aggregation of the track occupancy	§Aggregation			§Resolved Movable Object Extent
Generic product Assurance	$APS shall be compliant with the safety requirements identified during the risk analysis				
Managing Configurations	$APS subsystem software approval must be possible independent of configuration data				
Safety Checks, Occupancy Claims Identifiable with Localisation Technologies, Life Cycle Cost, Standardised interfaces	$APS support different ETCS system versions within the same APS Area of Control				
Managing Warning Areas	$Before granting a movement, APS must secure that the configured maximum pre-warning time is not violated			§MP in relation with WA	
Managing Configurations	$Build a system that is capable of handling the highest RAMS and non-functional Requirements of an IM				
Managing Configurations	$Default configuration shall contain values which can be changed within an unambiguously defined range to adapt to an IM's requirements				
Managing Configurations	$Define formal values / value ranges for each RAMS and non-functional requirement in combination with the corresponding runtime environment (e.g. hardware, operating system)				
Safety Checks	$Each safety condition APS check shall be unambiguously specified				

Safety Checks	$Each safety condition violation, identified by APS, shall be unambiguously specified				
Safety Checks	$Each safety measure, APS and its resulting safety condition cause, shall be unambiguously specified				
Life Cycle Cost	$Ensure an agreed and committed life cycle policy between all suppliers for investment protection				
Safety Checks, Standardised interfaces, Functional independency	$Ensure clear layering for transport, marshalling and application model				
Generic product Assurance	$Ensure safety relevance of each component to prevent components from suddenly becoming safety relevant in a later implementation				
Life Cycle Cost	$Future sematic changes shall under no circumstance require changes in the interfaces				
Managing Configurations	$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				
Standardised interfaces	$No participant may claim any rights to the APS specifications or further work results openly published under the agreed open-source licence				
Life Cycle Cost	$Provide quantities and frequencies of processed data towards Monitoring	§Measurement			
Life Cycle Cost	$Provisioning of measurement data must not influence the performance of APS				
Independency from Project Planning, Generic product Assurance	$Safety checks shall be independent of operational procedures				
Independency from Project Planning, Functional independency	$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 Movable Objects Concept - Solution Details
Managing Configurations	$Support the identification of an incompatible version/built for each layer (transport, marshalling, application model) during any installation procedure				
Safety Checks, Functional independency	$The behaviour of the individual APS components shall be unambiguously specified				
Standardised interfaces	$The behaviour of the individual APS components should be formally specified when required by formal validation				
Independency from Project Planning, Generic product Assurance, Functional independency	$The combined use of functional building blocks shall not require an additional safety assurance				
Managing Configurations, Independency from Project Planning	$The definition and configuration of safety conditions to be checked by APS shall not contain site or location specific references				
Generic product Assurance	$The safety processes of the APS solution design (supplier activities) and the APS concept design (IM activities) shall be aligned				
Standardised interfaces	$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				
Occupancy Claims Identifiable with Localisation Technologies	$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	§Aggregation			§Resolved Movable Object Extent

Life Cycle Cost	$Within the Area of Control, APS shall support minimally 1250 switchable field elements		§Set switchable field elements		
Life Cycle Cost	$Within the Area of Control, APS shall support minimally 3.000 TTD				
Life Cycle Cost	$Within the Area of Control, APS shall support the safe production of minimum of 75 simultaneous train units (moving, stopped) per hour				